

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-159074  
 (43)Date of publication of application : 31.05.2002

(51)Int.CI.

H04Q 9/00  
 G06F 13/00  
 G06F 15/00  
 H04M 11/00  
 H04N 5/00

(21)Application number : 2000-350956

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

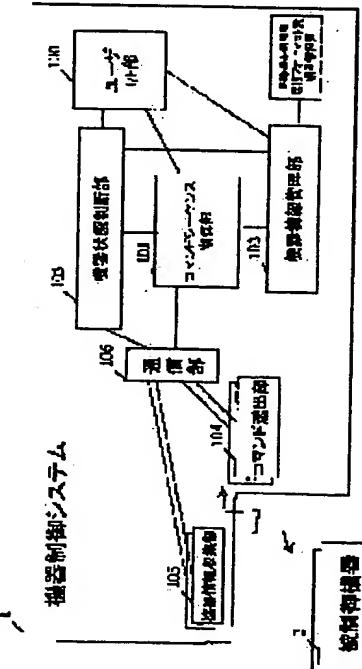
(22)Date of filing : 17.11.2000

(72)Inventor : KOKADO TAKESHI

## (54) EQUIPMENT CONTROL SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To surely and remotely control conventional household electric equipment.  
**SOLUTION:** An equipment control system comprises an equipment information collector 105 for collecting information of a phenomenon occurring by an operation of equipment 2 to be controlled. The system further comprises an equipment state deciding unit 103 for inferring a state of each equipment 2 to be controlled from the collected information capable of remotely knowing the state of the conventional household electric equipment (the equipment having only a receiving function of a remote control signal or the equipment even having no receiving function of the signal). The system also comprises a command sequence controller 101 for designating sending of the remote control signal while referring to the state of the equipment 2 from the deciding unit 103 to enable a remote control with high reliability.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP) (12) 公開特許公報 (A) (11)特許出願公開番号  
 特開2002-159074  
 (P2002-159074A)

(43)公開日 平成14年5月31日 (2002.5.31)

(51)IntCl'	識別記号	F I	マークコード(参考)
H 04 Q 9/00	3 0 1	H 04 Q 9/00	3 0 1 D 5 B 0 8 5
G 06 F 13/00	3 5 7	G 06 F 13/00	3 0 1 E 5 B 0 8 9
15/00	3 1 0	15/00	3 5 7 A 5 C 0 5 6
H 04 M 11/00	3 0 1	H 04 M 11/00	3 1 0 E 5 K 0 4 8
			3 0 1 5 K 1 0 1

審査請求 未請求 請求項の数30 OL (全32頁) 最終頁に統く

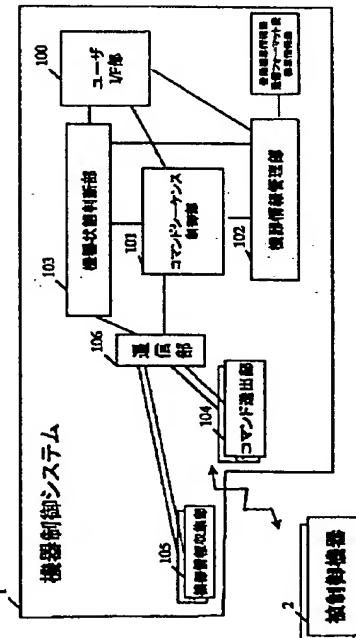
(21)出願番号	特願2000-350956(P2000-350956)	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成12年11月17日 (2000.11.17)	(72)発明者	古門 健 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(74)代理人	100097445 弁理士 岩橋 文雄 (外2名)
			最終頁に統く

(54)【発明の名称】 機器制御システム

(57)【要約】

【課題】 従来の家電を遠隔から確実に制御することを目的とする。

【解決手段】 被制御機器2の動作によって生じた現象の情報を収集する機器情報収集部105を設ける。そして、機器状態判断部103が収集した情報から各被制御機器2の状態を推測することにより、従来家電（リモコン信号の受信機能しかない機器又は、リモコン信号の受信機能を持たない機器）の状態を遠隔から知ることが可能となる。また、コマンドシーケンス制御部101が、機器状態判断部103より各被制御機器2の状態を参照しながらリモコン信号の送出を指示することにより信頼性の高い遠隔制御が可能となる。



【特許請求の範囲】

【請求項 1】被制御機器にコマンドを送信するコマンド送信手段と、

前記被制御機器の外部から被制御機器の動作によって生じる物理現象情報を収集する機器情報収集手段と、前記機器情報収集手段を通じて得た情報から被制御機器の状態を判断する機器状態判断手段と、

前記機器状態判断手段が判断した機器の状態に基づき、被制御機器に対するコマンド送出シーケンスを決定し、前記コマンド送信手段にコマンド送信を指示するコマンドシーケンス制御手段とを備えたことを特徴とする機器制御システム。

【請求項 2】前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信を指示した後、前記機器状態判断手段より被制御機器の状態を取得し、被制御機器に対するコマンド送出シーケンスを決定することを特徴とする請求項 1 記載の機器制御システム。

【請求項 3】前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信を指示した後、前記機器状態判断手段より被制御機器の状態を取得し、期待される状態への遷移が検出されない場合、再度、前記コマンド送信手段にコマンド送信を指示することを特徴とする請求項 2 記載の機器制御システム。

【請求項 4】前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信を指示した後、規定の時刻に前記機器状態判断手段より被制御機器の状態を取得し、期待される状態への遷移が検出されない場合、前記コマンド送信手段にコマンド送信を指示することを特徴とする請求項 2 記載の機器制御システム。

【請求項 5】前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信の指示を規定回数行っても、被制御機器の状態が期待される状態へ遷移しない場合、

前記コマンドシーケンス制御手段が、障害通知処理を起動することを特徴とする請求項 2 から請求項 4 のいずれかに記載の機器制御システム。

【請求項 6】被制御機器の動作によって生じる物理現象の情報を収集する機器情報収集手段と、

前記機器情報収集手段を通じて得た情報から被制御機器の状態を判断する機器状態判断手段と、

前記被制御機器にコマンドを送信するコマンド送信手段と、

前記機器状態判断手段が判断した機器の状態に基づき、被制御機器に対するコマンド送出シーケンスを決定し、前記コマンド送信手段にコマンド送信を指示するコマンドシーケンス制御手段と、

機器制御システムへの新たな被制御機器の登録時に、被制御機器に関する情報を受け取る機器登録受付手段と、前記機器登録受付手段より被制御機器に関する情報を受け取り、機器制御システムに登録された被制御機器の情

報を管理する機器情報管理手段とを備え、

前記情報管理手段が、新たな被制御機器を登録する時、被制御機器の情報を受け取った前記機器登録受付手段の識別により、被制御機器へコマンド発行可能なコマンド送出手段を判断し、前記コマンド送出手段と被制御機器の情報とを関連付けて管理することを特徴とする請求項 1 から請求項 5 のいずれかに記載の機器制御システム。

【請求項 7】機器制御システムに新たな被制御機器を登録する時、

前記機器登録受付手段に対して被制御機器用のリモコン信号発生機が送出するリモコン信号を入力し、

前記機器情報管理手段が、前記機器登録受付手段が受信したリモコン信号を解析して被制御機器の情報を設定することを特徴とする請求項 6 記載の機器制御システム。

【請求項 8】機器制御システムに新たな被制御機器を登録する時、

前記機器登録受付手段に対して被制御機器用のリモコン信号発生機が送出するリモコン信号が入力されると、

前記機器情報管理手段が、前記被制御機器の情報を収集する前記機器情報収集手段の登録要求をユーザーに通知し、

ユーザーが前記機器情報収集手段の登録を行うと、前記機器情報管理手段が、登録された前記機器情報収集手段と被制御機器の情報をとを関連付けて管理することを特徴とする請求項 7 記載の機器制御システム。

【請求項 9】前記機器情報収集手段が被制御機器に流れれる電流量、被制御機器の消費電力量のような電気的情報を検出することを特徴とする請求項 1 から請求項 8 のいずれかに記載の機器制御システム。

【請求項 10】前記機器情報収集手段が被制御機器の発する光、音、風、温度を検出することを特徴とする請求項 1 から請求項 8 のいずれかに記載の機器制御システム。

【請求項 11】前記機器情報収集手段が被制御機器の振動、加速度、移動速度のような被制御機器の力学的運動を検出することを特徴とする請求項 1 から請求項 8 のいずれかに記載の機器制御システム。

【請求項 12】前記機器情報収集手段は、被制御機器の電源プラグを接続するための差込口と、コンセントに差し込むための突起部を備えることを特徴とする請求項 9 記載の機器制御システム。

【請求項 13】前記機器情報収集手段は、被制御機器の電源プラグを接続する差込口に流れる電流のON、OFF を前記コマンド送信手段の指示により行うことを特徴とする請求項 12 記載の機器制御システム。

【請求項 14】機器情報収集手段を通じて得た情報から被制御機器の状態を判断する機器状態判断手段と、前記機器状態判断手段が判断した機器の状態に基づき、被制御機器に対するコマンド送出シーケンスを決定し、前記コマンド送信手段にコマンド送信を指示するコマンドシ

一ケンス制御手段と、機器制御システムに登録されている被制御機器の情報と被制御機器へのコマンド送出を行うコマンド送出手段とを関連付けて管理する機器情報管理手段と、制御子機部との通信を制御する宅内通信手段とを備えた制御親機部と、

制御親機部との通信を制御する宅内通信手段と、被制御機器にコマンドを送信するコマンド送信手段と、機器制御システムへの新たな被制御機器の登録時に、被制御機器に関する情報を受け取る機器登録受付手段とを備えた制御子機部と、

被制御機器の動作によって生じる現象の情報を収集する機器情報収集手段とを備えたことを特徴とする請求項1から請求項13のいずれかに記載の機器制御システム。

【請求項15】前記制御子機部は、電灯の電源プラグを接続するための差込口と、電灯用コンセントに差し込むための突起部を備えることを特徴とする請求項14記載の機器制御システム。

【請求項16】前記制御子機部は、前記制御子機部本体に支持部を設け、支持部に被制御機器へのコマンドを発射するコマンド送出素子、または新たな被制御機器の登録時に被制御機器に関する情報信号を受信する登録信号受信素子、或いは前記コマンド送出素子と前記登録信号受信素子の両方を取り付けたことを特徴とする請求項15記載の機器制御システム。

【請求項17】ユーザ端末を用いて遠隔から被制御機器を制御可能な機器制御システムにおいて、インターネットを通じた通信を行うインターネットアクセス手段と、

回線交換網を用いた通信を行う電話網アクセス手段と、前記電話網アクセス手段から得る通信情報をもとに、通信相手の認証を行う通信情報解析手段と、

前記インターネットアクセス手段に接続され、インターネットアクセス手段を介してユーザ端末と被制御機器との通信を制御する機器制御手段とを備え、

前記通信情報解析手段が認証結果に基づき、前記インターネットアクセス手段の通信条件を決定し、前記インターネットアクセス手段の通信条件を変更させることを特徴とする機器制御システム。

【請求項18】前記電話網アクセス手段への着呼する

と、  
前記通信情報解析手段が前記電話網アクセス手段の通信先の認証を行い、認証に合格した場合、前記通信情報解析手段が、ユーザ端末がインターネットを通じてアクセス可能となるように前記インターネットアクセス手段の通信条件を変更させ、

前記通信情報解析手段が前記通信条件を変更させた後、規定された時間経過したか、又は認証されたユーザ端末がインターネットを通じた通信を終了した場合、

前記インターネットアクセス手段の前記通信条件を前記通信情報解析手段による変更前の状態に戻すことを特徴

とする請求項17記載の機器制御システム。

【請求項19】前記通信情報解析手段が設定させるインターネットアクセス手段の通信条件がパケットフィルタリングの設定であることを特徴とする請求項18記載の機器制御システム。

【請求項20】前記通信情報解析手段が、ユーザ端末がインターネットを通じてアクセス可能となるように前記インターネットアクセス手段の通信条件を変更させることにより、前記インターネットアクセス手段がダイヤルアップによりインターネットに接続し、

前記インターネットアクセス手段の前記通信条件を前記通信情報解析手段の変更前の状態に戻すことにより、ダイヤルアップによるインターネットとの接続を切断することを特徴とする請求項17から請求項19のいずれかに記載の機器制御システム。

【請求項21】前記通信情報解析手段が、電話網アクセス手段から得る情報を処理することで特定される相手先に対して、

インターネットを用いて機器制御システムへアクセスするためのアドレス情報を電子メールにより通知することを特徴とする請求項17から請求項20のいずれかに記載の機器制御システム。

【請求項22】前記電話網アクセス手段への着呼時に、発呼元が前記インターネットアクセス手段にアクセスするときに用いるユーザ端末のアドレス情報を通知し、前記通信情報解析手段が、通知されたアドレス情報を用いて、ユーザ端末が機器制御システムにアクセスが行えるようにインターネットアクセス手段のファイアウォールを設定することを特徴とする請求項19記載の機器制御システム。

【請求項23】前記通信情報解析手段が認証の結果に基づき、前記インターネットアクセス手段の通信条件が設定された後、インターネットから前記インターネットアクセス手段を介して前記機器制御システムへのアクセスが発生した時、

最初に前記機器制御システムへのアクセスを行った発信元以外のアクセスを受け付けないように、前記インターネットアクセス手段のファイアウォールを設定することを特徴とする請求項17から請求項21のいずれかに記載の機器制御システム。

【請求項24】前記インターネットアクセス手段を介してアクセスしている外部端末が、所定の操作を行うことで、前記電話網アクセス手段への着呼後に設定された前記インターネットアクセス手段の通信条件を着呼前の状態に再度戻すことを特徴とする請求項17から請求項23のいずれかに記載の機器制御システム。

【請求項25】前記電話網アクセス手段への着呼により、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から通信先の情報を得て認証を行い、認

証結果に基づき、前記インターネットアクセス手段を通じて外部からアクセスする時のサービスクラス、又は制御可能な機器、或いはその両方が決定されることを特徴とする請求項17から請求項24のいずれかに記載の機器制御システム。

【請求項26】機器制御システムへインターネットを通じたアクセスを開始する時に実行されるログイン処理において、

前記インターネットアクセス手段が外部ユーザからのログイン要求を受け取った時、前記通信情報解析手段がログイン許可を前記インターネットアクセス手段に与えるまで、ログイン処理を保留させ、

前記外部ユーザが前記電話網アクセス手段へ発呼し、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から通信先（外部ユーザ）の情報を得て認証を行い、通信先情報からユーザを特定し、特定されたユーザのログイン許可を前記インターネットアクセス手段に指示し、

前記インターネットアクセス手段がログイン処理を完了させることを特徴とする請求項17記載の機器制御システム。

【請求項27】前記インターネットアクセス手段がログインを保留させる時、前記外部ユーザの端末に対して、前記電話網アクセス手段へ回線交換網を用いた発呼を行わせるマークアップ言語で記述された情報を送信することを特徴とする請求項26記載の機器制御システム。

【請求項28】機器制御システムへインターネットを通じたアクセスを開始する時に実行されるログイン処理において、

外部ユーザのログイン名を受け取り、且つ、ログイン処理が完了していない状態で、前記通信情報解析手段がログインを保留させた上、前記インターネットアクセス手段を通じて認証用情報を前記外部ユーザに通知し、前記電話網アクセス手段への外部ユーザからの着呼を受け、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から通信先の情報を得て認証を行い、

さらに、前記通信情報解析手段が前記電話網アクセス手段を通じて通信先端末から、前記認証用情報そのもの又は、前記認証用情報に対して予め前記機器制御システムと申し合わせてある所定の処理を施した情報を受け取り、前記情報を認証した上、ログイン可能とするユーザを特定し、

特定されたユーザのログイン保留を解除し、ログインを完了させ、外部ユーザのインターネットを通じた前記機器制御システムへのアクセスを可能させることを特徴とする請求項17記載の機器制御システム。

【請求項29】前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から受け取る通信先の情報が、通信先の電話番号、端末番号、位置情報、基地局

IDであることを特徴とする請求項17から請求項28のいずれかに記載の機器制御システム。

【請求項30】請求項1から請求項16のいずれかに記載の機器情報収集手段とコマンド送信手段とコマンドシーケンス制御手段と機器登録受付手段と機器情報管理手段と、

請求項17から請求項29のいずれかに記載のインターネットアクセス手段と電話網アクセス手段と通信情報解析手段とを備えたことを特徴とする機器制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、離れた場所から機器の動作を制御することを可能とする機器制御システムに関する。

【0002】

【従来の技術】従来、家電のような機器を制御するため赤外線リモコンが使用されている。このようなりモコンでは、赤外線が同一室内でないと届かない点と、機器からの応答をリモートで受信する方法が用意されていない点から同一室内でユーザが機器の状態を監視しながらでないと使用できないものであった。

【0003】赤外線が同一室内でないと届かない問題点の解決方法としては、実開平5-31419号公報、特開平9-69885号公報、特開平9-270861号公報に記載されたものが知られている。これらは、リモコン信号送出機に通信手段を接続し、通信網を介して遠隔からリモコン信号送出を制御可能としたものである。しかし、家電のような機器では、赤外線リモコンによる制御は片方向であり、家電機器から応答を受信する方法がない。そのため、遠隔から機器を制御した場合、実際に機器が動作しているのか、動作していないのかを確認する手段がないという問題点がある。さらに、通信網としては基本的に電話網を前提としているため、遠くの機器を操作したい場合や操作が複雑で時間がかかる場合には、通信費コストが大きくなるという問題がある。さらに、通信網を介して遠隔から操作可能とした場合、第三者の不正アクセスによる機器操作を防ぐ必要がある。

【0004】この機器からの応答を受信するための解決方法としては、特開平9-18974号公報に記載されたものが知られている。先行特許では、被制御機器に対する赤外線リモコン信号を受信し、機器の状態を推定し蓄積する機器を設けることで、被制御機器の状態を検出可能とする。しかし、本方法は被制御機器に入力されたリモコン信号から被制御機器の状態を推定しているに過ぎず、被制御機器がリモコン信号の受信誤りや電源が入っていない等の理由で予測外の動作を行った場合、推定された状態との不一致が発生し、その不一致に気づかないという問題点がある。なお、先行特許でも前記問題点については、HA端子を用いた解決方法について述べられているが、HA端子は一部の家電に採用されているだ

けであり、大部分の家電では使用できない。

【0005】通信費コストが大きくなるという問題については、インターネットを使用することが考えられる。インターネットを使用することで、常時接続されている環境であれば機器制御のための通信費は必要なくなる。また、常時接続されていない環境でも、被制御機器との距離が非常に離れている場合等には、大きな通信費削減が期待できる。さらに、外部からのアクセス端末のユーザ・インターフェースをWWWブラウザで実現することで、専用の端末を準備することなく、分かり易いインターフェースをユーザに提供することが可能となる。

【0006】また、第三者の不正アクセスを防ぐ方法としては、特開平10-341224号公報、特開2000-10927号公報に記載されたものが知られている。特開平10-341224号公報に記載されたものは、ユーザが通信網を介してシステムにログインする場合に、まず、システムに対して自分の識別情報を入力する。そして、システムは、トランザクション番号(TAN)をユーザが識別情報を入力した伝送路とは、別の伝送路を用いてユーザに送信し、このTANを受信したユーザは、それを再び、システムに入力することでシステムが認証を実行し、ログインが完了するものである。しかし、本方式では不正アクセス者が識別情報の入力まで成功すると、必ずTANが送信されることになり、TANを盗むタイミングを不正アクセス者がコントロールすることができるため、TANを盗まれ不正アクセスが成功する可能性が高くなるという問題がある。

【0007】一方、特開2000-10927号公報に記載されたものは、ユーザが携帯電話端末からパスワードを付けて、システムに対して発呼し、それを受けたシステムは、発呼元の電話番号とパスワードからユーザを認証した上、一時的なパスワードをユーザの携帯電話端末に送信する。ユーザは、PCからその一時的なパスワードを用いてシステムにログインするというものである。本方式でも通信路を介したパスワードの送信が行われるため、パスワードが盗聴され、ユーザのログインより先に、盗聴したパスワードを用いて不正にログインされる危険性がある。

【0008】さらに、特開平10-341224号公報、特開2000-10927号公報に記載されたどちらのものも、本質は一時的に使用できる認証用情報の受け渡しにあり、この認証用情報の入手困難さでシステムへの不正アクセスを防ぐというものである。従って、機器制御システムをインターネットを介して制御可能とするために、特開平10-341224号公報、特開2000-10927号公報に記載されたものを採用した場合には、パスワード(認証用情報)の漏洩による不正アクセスには効果的であると考えられるが、現状インターネットで問題になっているOSやアプリケーションのバグを利用する不正アクセスへの効果的対策にはならない

可能性がある。静止画のような連続性を必要としないデータを扱うサーバ装置では、データの入出力をを行う場合、実際にデータの入出力実行する時に使用可能なリソースを用いてデータの入出力が実行される。

【0009】

【発明が解決しようとする課題】この機器制御システムは、従来の家電を含む機器を遠隔から確実に制御することができ、且つ、第三者の不正な制御を禁止することができる要求されている。

【0010】本発明は、従来の家電機器の動作情報を収集することで、機器の制御を確実に行うことを可能とし、また、外部からインターネットを通じて安全にアクセス可能とした機器制御システムの提供を目的とする。

【0011】

【課題を解決するための手段】この課題を解決するため第1の発明の機器制御システムでは、被制御機器にコマンドを送信するコマンド送信手段と、前記被制御機器の外部から被制御機器の動作によって生じる物理現象情報を収集する機器情報収集手段と、前記機器情報収集手段を通じて得た情報から被制御機器の状態を判断する機器状態判断手段と、前記機器状態判断手段が判断した機器の状態に基づき、被制御機器に対するコマンド送出シーケンスを決定し、前記コマンド送信手段にコマンド送信を指示するコマンドシーケンス制御手段とを備える。この構成によって、従来の電気機器のように赤外線リモコンによる片方向の通信機能しか持たない機器においても、機器情報収集手段が被制御機器の動作状況の情報を収集し、機器状態判断手段に報告することで、機器状態判断手段が機器の状態を推定することが可能となり、機器の状態に応じた制御が可能となる。

【0012】第2の発明の機器制御システムでは、第1の発明の前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信を指示した後、前記機器状態判断手段より被制御機器の状態を取得し、被制御機器に対するコマンド送出シーケンスを決定する。この制御により、機器制御の確実性を向上させることができる。

【0013】第3の発明の機器制御システムでは、第2の発明の前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信を指示した後、前記機器状態判断手段より被制御機器の状態を取得し、期待される状態への遷移が検出されない場合、再度、前記コマンド送信手段にコマンド送信を指示することを特徴とする。この制御により、機器制御の確実性を向上させることができる。

【0014】第4の発明の機器制御システムでは、第2の発明の前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信を指示した後、規定の時刻に前記機器状態判断手段より被制御機器の状態を取得し、期待される状態への遷移が検出されない場合、前記

コマンド送信手段にコマンド送信を指示することを特徴とする。この制御により、タイマを利用した制御を行った場合の信頼性を向上させることができる。

【0015】第5の発明の機器制御システムでは、第2から第4の発明の前記コマンドシーケンス制御手段が、前記コマンド送信手段にコマンド送信の指示を規定回数行っても、被制御機器の状態が期待される状態へ遷移しない場合、前記コマンドシーケンス制御手段が、障害通知処理を起動することを特徴とする。これにより、ユーザが機器制御が失敗したことを探ることが可能となる。

【0016】第6の発明の機器制御システムでは、被制御機器の動作によって生じる物理現象の情報を収集する機器情報収集手段と、前記機器情報収集手段を通じて得た情報から被制御機器の状態を判断する機器状態判断手段と、前記被制御機器にコマンドを送信するコマンド送信手段と、前記機器状態判断手段が判断した機器の状態に基づき、被制御機器に対するコマンド送出シーケンスを決定し、前記コマンド送信手段にコマンド送信を指示するコマンドシーケンス制御手段と、機器制御システムへの新たな被制御機器の登録時に、被制御機器に関する情報を受け取る機器登録受付手段と、前記機器登録受付手段より被制御機器に関する情報を受け取り、機器制御システムに登録された被制御機器の情報を管理する機器情報管理手段とを備え、前記機器情報管理手段が、新たな被制御機器を登録する時、被制御機器の情報を受け取った前記機器登録受付手段の識別により、被制御機器へコマンド発行可能なコマンド送出手段を判断し、前記コマンド送出手段と被制御機器の情報を関連付けて管理することを特徴とする。この処理によって、離れた場所に同一の被制御機器（例えば同一型式のビデオ）が存在する場合、両者を区別して制御することができる。

【0017】第7の発明の機器制御システムでは、機器制御システムに新たな被制御機器を登録する時、前記機器登録受付手段に対して被制御機器用のリモコン信号発生機が送出するリモコン信号を入力し、前記機器情報管理手段が、前記機器登録受付手段が受信したリモコン信号を解析して被制御機器の情報を設定することを特徴とする。この制御により、被制御機器の新規登録を簡単化することができる。

【0018】第8の発明の機器制御システムでは、機器制御システムに新たな被制御機器を登録する時、前記機器登録受付手段に対して被制御機器用のリモコン信号発生機が送出するリモコン信号が入力されると、前記機器情報管理手段が、前記被制御機器の情報を収集する前記機器情報収集手段の登録要求をユーザに通知し、ユーザが前記機器情報収集手段の登録を行うと、前記機器情報管理手段が、登録された前記機器情報収集手段と被制御機器の情報を関連付けて管理することを特徴とする。この制御により、被制御機器と機器情報収集手段とを関連付けることができる。

【0019】第9の発明の機器制御システムでは、前記機器情報収集手段が被制御機器に流れる電流量、被制御機器の消費電力量のような電気的情報を検出することを特徴とする。この構成により、機器情報収集手段は、被制御機器の電気的情報を収集することが可能となる。

【0020】第10の発明の機器制御システムでは、前記機器情報収集手段が被制御機器が発する光、音、風、温度を検出することを特徴とする。この構成により、機器情報収集手段は被制御機器が発する光、音、風、温度の情報を検出することが可能となる。

【0021】第11の発明の機器制御システムでは、前記機器情報収集手段が被制御機器の振動、加速度、移動速度のような被制御機器の力学的運動を検出することを特徴とする。この構成により、機器情報収集手段は被制御機器の力学的運動を検出することが可能となる。

【0022】第12の発明の機器制御システムでは、機器情報収集手段が、被制御機器の電源プラグを接続するための差込口と、コンセントに差し込むための突起部を備えることを特徴とする。この構成により、機器情報収集手段が容易に被制御機器に関する電気的情報を得ることが可能となる。

【0023】第13の発明の機器制御システムでは、機器情報収集手段が、被制御機器の電源プラグを接続する差込口に流れる電流のON、OFFを前記コマンド送信手段の指示により行うことを特徴とする。この構成により、被制御機器の電源の制御を被制御機器のリモコンに頼らずに行うことが可能となる。

【0024】第14の発明の機器制御システムでは、機器情報収集手段を通じて得た情報から被制御機器の状態を判断する機器状態判断手段と、前記機器状態判断手段が判断した機器の状態に基づき、被制御機器に対するコマンド送信シーケンスを決定し、前記コマンド送信手段にコマンド送信を指示するコマンドシーケンス制御手段と、機器制御システムに登録されている被制御機器の情報と被制御機器へのコマンド送出を行うコマンド送出手段とを関連付けて管理する機器情報管理手段と、制御子機部との通信を制御する宅内通信手段とを備えた制御親機部と、制御親機部との通信を制御する宅内通信手段と、被制御機器にコマンドを送信するコマンド送信手段と、機器制御システムへの新たな被制御機器の登録時に、被制御機器に関する情報を受け取る機器登録受付手段とを備えた制御子機部と、被制御機器の動作によって生じる現象の情報を収集する機器情報収集手段とを備えたことを特徴とする。この構成によって、各部屋に設置された被制御機器を制御することが容易になる。

【0025】第15の発明の機器制御システムでは、制御子機部は、電灯の電源プラグを接続するための差込口と、電灯用コンセントに差し込むための突起部を備えることを特徴とする。この構成により、部屋内を見通せる場所に制御子機を取り付けることが可能となり、結果と

して被制御機器に対してリモコン信号送信が容易となる。

【0026】第16の発明の機器制御システムでは、前記制御子機部本体に支持部を設け、前記支持部に被制御機器へのコマンドを発射するコマンド送出素子、または新たな被制御機器の登録時に被制御機器に関する情報信号を受信する登録信号受信素子、或いは前記コマンド送出素子と前記登録信号受信素子の両方を取り付けたことを特徴とする。この構成によって、電灯に邪魔されずにリモコン信号の送出、登録信号の受信を行うことが可能となる。

【0027】第17の発明の機器制御システムでは、ユーザ端末を用いて遠隔から被制御機器を制御可能な機器制御システムにおいて、インターネットを通じた通信を行うインターネットアクセス手段と、回線交換網を用いた通信を行う電話網アクセス手段と電話網アクセス手段から得る通信情報をもとに、通信相手の認証を行う通信情報解析手段と、前記インターネットアクセス手段に接続され、インターネットアクセス手段を介してユーザ端末と被制御機器との通信を制御する機器制御手段とを備え、前記通信情報解析手段が認証結果に基づき、前記インターネットアクセス手段の通信条件を決定し、前記インターネットアクセス手段の通信条件を変更させることを特徴とする。この構成により、回線交換網から得る通信情報により相手先を認証した結果により、インターネットアクセス手段の通信条件が設定されるため、セキュリティを向上させることが可能となる。

【0028】第18の発明の機器制御システムでは、前記電話網アクセス手段への着呼すると、前記通信情報解析手段が前記電話網アクセス手段の通信先の認証を行い、認証に合格した場合、前記通信情報解析手段が、ユーザ端末がインターネットを通じてアクセス可能となるように前記インターネットアクセス手段の通信条件を変更させ、前記通信情報解析手段が前記通信条件を変更させた後、規定された時間経過したか、又は認証されたユーザ端末がインターネットを通じた通信を終了した場合、前記インターネットアクセス手段の前記通信条件を前記通信情報解析手段による変更前の状態に戻すことを特徴とする。この制御によって、インターネットを通じた正規ユーザーのアクセス終了後、インターネットアクセス手段の通信条件がリセットされることになり、インターネットを通じた不正アクセスを困難にさせることが可能となる。

【0029】第19の発明の機器制御システムでは、前記通信情報解析手段が設定させるインターネットアクセス手段の通信条件がパケットフィルタリングの設定であることを特徴とする。この構成により、パケットフィルタリングにより、不正アクセスを防ぐことが可能になる。

【0030】第20の発明の機器制御システムでは、前

記通信情報解析手段が、ユーザ端末がインターネットを通じてアクセス可能となるように前記インターネットアクセス手段の通信条件を変更させることにより、前記インターネットアクセス手段がダイヤルアップによりインターネットに接続し、前記インターネットアクセス手段の前記通信条件を前記通信情報解析手段の変更前の状態に戻すことにより、ダイアルアップによるインターネットとの接続を切断することを特徴とする。このような制御により、常に、インターネットに接続されていない機器制御システムをインターネットを介して制御することが可能となる。

【0031】第21の発明の機器制御システムでは、前記通信情報解析手段が、電話網アクセス手段から得る情報を処理することで特定される相手先に対して、インターネットを用いて機器制御システムへアクセスするためのアドレス情報を電子メールにより通知することを特徴とする。この制御により、機器制御システムのアドレスが変化する構成においても、インターネットを通じて機器制御システムにアクセスするユーザが、機器制御システムのアクセス用アドレスを知ることが可能となる。

【0032】第22の発明の機器制御システムでは、前記電話網アクセス手段への着呼時に、発呼元が前記インターネットアクセス手段にアクセスするときに用いるユーザ端末のアドレス情報を通知し、前記通信情報解析手段が、通知されたアドレス情報を用いて、ユーザ端末が機器制御システムにアクセスが行えるようにインターネットアクセス手段のファイアウォールを設定することを特徴とする。この制御により、ユーザ端末のアドレスが変化する構成においても、インターネットアクセス手段のパケットフィルタリング設定等のファイアウォールの設定を有効に行うことができる。

【0033】第23の発明の機器制御システムでは、前記通信情報解析手段が認証の結果に基づき、前記インターネットアクセス手段の通信条件が設定された後、インターネットから前記インターネットアクセス手段を介して前記機器制御システムへのアクセスが発生した時、最初に前記機器制御システムへのアクセスを行った発信元以外のアクセスを受け付けないように、前記インターネットアクセス手段のファイアウォールを設定することを特徴とする。この制御により、ユーザ端末のアドレスが変化する構成においても、正規ユーザーアクセス後は不正なユーザのアクセスが防止されるため、不正アクセスを効果的に防ぐことが可能となる。

【0034】第24の発明の機器制御システムでは、前記インターネットアクセス手段を介してアクセスしている外部端末が、所定の操作を行うことで、前記電話網アクセス手段への着呼後に設定された前記インターネットアクセス手段の通信条件を着呼前の状態に再度戻すことを特徴とする。この制御により、正規ユーザーがインターネットを通じたアクセスの終了時、明示的にインターネ

ットアクセス手段の通信条件をリセットし、インターネットを通じた外部からのアクセスを禁止させることができる。能となるためセキュリティを向上させることができる。

【0035】第25の発明の機器制御システムでは、前記電話網アクセス手段への着呼により、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から通信先の情報を得て認証を行い、認証結果に基づき、前記インターネットアクセス手段を通じて外部からアクセスする時のサービスクラス、又は制御可能な機器、或いはその両方が決定されることを特徴とする。本制御により、管理者の認証情報させ厳重に管理しておけば、仮に他のユーザーとして機器制御システムへの不正侵入に成功したとしても、サービスクラスや制御可能な機器等の制限をかけることが可能なため、セキュリティを向上させることができる。

【0036】第26の発明の機器制御システムでは、機器制御システムへインターネットを通じたアクセスを開始する時に実行されるログイン処理において、前記インターネットアクセス手段が外部ユーザーからのログイン要求を受け取った時、前記通信情報解析手段がログイン許可を前記インターネットアクセス手段に与えるまで、ログイン処理を保留させ、前記外部ユーザーが前記電話網アクセス手段へ発呼し、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から通信先（外部ユーザー）の情報を得て認証を行い、通信先情報からユーザーを特定し、特定されたユーザーのログイン許可を前記インターネットアクセス手段に指示し、前記インターネットアクセス手段がログイン処理を完了させることを特徴とする。この制御により、回線交換網から通信先（外部ユーザー）の情報を得た認証に合格できなければ、インターネットを通じたアクセスログイン処理が行われないため、不正アクセスが困難となりセキュリティが向上する。

【0037】第27の発明の機器制御システムでは、前記インターネットアクセス手段がログインを保留させる時、前記外部ユーザーの端末に対して、前記電話網アクセス手段へ回線交換網を用いた発呼を行わせるマークアップ言語で記述された情報を送信することを特徴とする。この制御により、前記通信情報解析手段がユーザー認証するために、ユーザーが機器制御システムの電話網アクセス手段へ発呼することが容易になる。

【0038】第28の発明の機器制御システムでは、機器制御システムへインターネットを通じたアクセスを開始する時に実行されるログイン処理において、外部ユーザーのログイン名を受け取り、且つ、ログイン処理が完了していない状態で、前記通信情報解析手段がログインを保留させた上、前記インターネットアクセス手段を通じて認証用情報を前記外部ユーザーに通知し、前記電話網アクセス手段への外部ユーザーからの着呼を受け、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線

交換網から通信先の情報を得て認証を行い、さらに、前記通信情報解析手段が前記電話網アクセス手段を通じて通信先端末から、前記認証用情報そのもの又は、前記認証用情報に対して予め前記機器制御システムと申し合せてある所定の処理を施した情報を受け取り、前記情報を認証した上、ログイン可能とするユーザーを特定し、特定されたユーザーのログイン保留を解除し、ログインを完了させ、外部ユーザーのインターネットを通じた前記機器制御システムへのアクセスを可能させることを特徴とする。この制御により、電話網アクセス手段より着呼び前記通信情報解析手段により認証されたユーザーと、インターネットを通じたアクセスユーザーを関連付けることが可能となり、インターネットを通じた機器制御システムへのアクセスのセキュリティが向上する。

【0039】第29の発明の機器制御システムでは、前記通信情報解析手段が前記電話網アクセス手段を通じて、回線交換網から受け取る通信先の情報が、通信先の電話番号、端末番号、位置情報、基地局IDであることを特徴とする。このような制御により、信情報解析手段が電話番号、端末番号、位置情報、基地局IDを認証に使用することが可能となり、機器制御システムのセキュリティが向上する。

【0040】第30の発明の機器制御システムでは、第1の発明から第16の発明の機器情報収集手段とコマンド送信手段とコマンドシーケンス制御手段と機器登録受付手段と機器情報管理手段と、第17の発明から第29の発明のインターネットアクセス手段と電話網アクセス手段と通信情報解析手段とを備えたことを特徴とする。この構成により、インターネットを通じた従来の赤外線による片方向の制御機能しかもたない機器の遠隔制御を、安全確実に行うことが可能となる。

【0041】

【発明の実施の形態】以下本発明の実施の形態について、図1から図5を用いて説明する。

【0042】（実施の形態1）図1は本発明の実施の形態1における機器制御システム機器の構成を示すものである。図1において、1は機器制御システム機器、2は機器制御システム機器1によって制御される被制御機器、100は機器制御システム機器のユーザーI/Fを提供するユーザーI/F部、101は機器制御のためのコマンド送出シーケンスを決定し、コマンド送出部104にコマンド送出を指示するコマンドシーケンス制御部、102は機器制御システム機器1の制御対象として登録されている被制御機器2の構成及び被制御機器のコマンド情報等を管理する機器情報管理部、103は機器情報管理部102が管理する機器の情報と機器情報収集部105から得られる情報を用いて被制御機器2の状態を判断する機器状態判断部、104は被制御機器に対してリモコン信号を送出するコマンド送出部、105は被制御機器の動作によって生じる現象の情報を収集する機器情報

収集部、106はコマンドシーケンス制御部101、機器状態判断部103と機器情報収集部105、コマンド送出部104との通信可能とさせる通信部である。

【0043】図2は登録機器情報表の一構成例を示すものである。登録機器構成表は、機器情報管理部102で管理され、機器制御システム機器1の制御対象として登録されている被制御機器2の情報が記載されたものである。登録機器情報表内の被制御機器名は、ユーザが被制御機器を識別するために使用される被制御機器2の名前である。ユーザI/Fを通じて、ユーザが被制御機器の制御を行う場合、制御したい機器を被制御機器名で識別する。

【0044】被制御機器種別は被制御機器2の種別を示す情報である。被制御機器種別により、被制御機器2の種別（メーカ名、型番等）が一意に識別され、後述する送信フォーマット表及び機器情報表（図3）を用いることで、被制御機器2の制御用コマンドとコマンド送信フォーマットや状態解析用情報を得ることができる。ここで、状態解析用情報は、機器状態判断部103が機器情報収集部105から得られた情報をもとに機器の状態を判断する際に参照される情報である。

【0045】機器情報収集部1Dは各被制御機器2の情報を収集する機器情報収集部105を識別するための情報であり、被制御機器と機器情報収集部の関連付けを表す。本情報により、各被制御機器2の情報を収集する機器情報収集部105が特定される。

【0046】コマンド送出部1Dは各被制御機器2へのコマンド送出を行うことが可能なコマンド送出部104を識別するための情報であり、被制御機器とコマンド送出部との関連付けを表す。本情報により、仮に送信フォーマットと制御用コマンドコードが一致する複数の被制御機器が存在した場合でも、各被制御機器が離れており、関連付けられるコマンド送出部104が異なれば正常に制御することが可能となる。

【0047】図3は機器情報管理部で管理される送信フォーマット表と機器情報表の一構成例を示している。送信フォーマット表は、各社の被制御機器2に対するリモコン信号のフォーマット（キャリア周波数、コード長、コードのフォーマット等の情報）を示す情報である。コマンドシーケンス制御部101は、本情報を参考することで、メーカや機器によって異なる各被制御機器のリモコン信号のフォーマットを知ることが可能となる。

【0048】機器情報表は、各被制御機器に固有の情報が記載される。送信フォーマット種別は、その被制御機器のリモコン信号のフォーマット種別を示している。送信フォーマット種別と送信フォーマット表を用いて、各制御機器のリモコン信号フォーマットを知ることができ。制御用コマンドコードは、各被制御機器のリモコン使用時の制御コマンドのコードを示している。例えば、電源のON/OFFのコマンドコードが「0020」で

ある等の情報が記載される。本情報により、制御内容に対応するリモコン用コマンドコードを知ることが可能となる。

【0049】状態解析用情報は、機器情報収集部105が収集した情報から被制御機器の状態を判断する時に用いる情報である。機器状態判断部103は、本情報を参照することにより機器情報収集部105が収集した情報から被制御機器2の状態を判断することが可能となる。状態解析用情報の一例としては、被制御機器の各状態（電源OFF、電源ON待機中、再生中等）での消費電力が示されている。機器情報収集部105が被制御機器2で現状消費される電力を測定することによって、機器状態判断部は、各被制御機器105の状態を推測することが可能となる。

【0050】図4の(a)、(b)は被制御機器2の消費電力量を計測する機器情報収集部105の構成例を示している。図4の機器情報収集部105は、被制御機器2と電源コンセントとの間に挿入され、被制御機器105が消費する電力を測定する機能を有する。以下、このような機器情報収集部105をコンセント型と呼ぶことにする。

【0051】ここで、図4の(a)と(b)との相違点は、被制御機器2の電源プラグを接続するための差込口と電源コンセントに差し込むための電源プラグ部が分離されているか、一体化されているかだけの違いである。コンセント型機器情報収集部105が測定した被制御機器の消費電力は、通信部106を通じて機器状態判断部103に送信される。機器情報収集部105と機器状態判断部103との通信は、電力線、赤外線、無線等を用いて行われる。また、コンセント型機器情報収集部105は、コマンドシーケンス制御部101からの指示より被制御機器2への電力提供のON、OFFを行うことができる。

【0052】図5は被制御機器2の状態を光センサーにより検出するための機器情報収集部105の構成例とビデオへの機器情報収集部105の適用例である。以下、このような機器情報収集部105を光センサー型と呼ぶことにする。ビデオでは、たいていの機種で録画や再生中にそれを示すLEDが点灯する。そこで、そのLEDの光が受信されるように、光センサー型機器情報収集部の光センサーをビデオに取り付ける。ここで、本実施の形態では光センサーは光を電流量として検出するものとし、LEDの発行を検出すると光センサーに流れる電流量が増えるものとする。このように、光センサーを取り付けることにより、機器状態判断部103は、機器情報収集部105から各光センサーの電流量を受信することで、被制御機器2の状態を判断することが可能となる。

【0053】図10は実施の形態1での被制御機器2、機器情報収集部105、コマンド送出部104の配置の一例を示している。コマンド送出部104は、赤外線に

よるリモコン信号を送出する機能部であり、部屋内の被制御機器2を見通せる位置に配置することで、複数の被制御機器2に対してリモコン信号を送信することが可能となる。しかし、赤外線信号は壁等の障害物を通り抜けることができないため、他の部屋の被制御機器2に対してリモコン信号を送信することはできない。機器情報収集部105は、基本的に各制御機器2に対して個別に取り付けられ、被制御機器2の動作によって生じる現象（消費電力、光、音、振動、加速度等）の情報を収集する。また、複数の機器情報収集部105を1つの被制御機器2に取り付け、より詳細な情報を収集する形態もあり得る。

【0054】以上のように構成された機器制御システム機器について、その動作を説明する。図8はユーザーが被制御機器2の現状態の問い合わせを行った場合のシーケンスを示している。

【0055】まず、ユーザーが状態を問い合わせる要求を行う（S81）。ユーザーから被制御機器2の現状態の問い合わせを受けたユーザI/F部100は、状態を取得したい被制御機器2の機器名を指定した上、機器状態判断部103に機器の状態を要求する（S82）。ユーザI/F制御部100からの要求を受けた機器状態判断部103は、機器情報管理部102が管理する登録機器情報表を用いて、指定された機器名の被制御機器2の情報を収集する機器情報収集部105を特定する（S83）。

【0056】そして、機器情報判断部103は特定した機器情報収集部105から被制御機器2に関する現在情報を取得する（S84）。取得した被制御機器2に関する情報と機器情報表の状態解析用情報から被制御機器2の状態を判断する（S85）。なお、機器状態判断部103が被制御機器の状態を判断する方法の詳細については後述する。状態の判断が完了した機器状態判断部103は、ユーザI/F部に被制御機器2の状態を応答する。被制御機器2の状態を取得したユーザI/F部は、ユーザに被制御機器2の状態を応答する（S86）。

【0057】このシーケンスにより、通常の電気機器（リモコンによる遠隔操作機能を有するが、自身の状態や応答を返す機能及びI/Fを持たない機器）に対しても、ユーザーがその機器（被制御機器）の状態をリモートで知る（ユーザI/F部を通じて知る）ことが可能となる。

【0058】図9はユーザーがユーザI/F部100を通じて被制御機器2の制御を要求した場合のシーケンスを示している。ユーザI/F部100を通じて、ユーザーが被制御機器2の制御を要求する（S9A1）。コマンドシーケンス制御部101は、まず、リトライ回数を初期化する（S9A2）。

【0059】次に、機器状態判断部103に被制御機器2の状態を問い合わせる。なお、機器状態判断部103

が被制御機器の状態を判断する方法は後述する。そして、コマンドシーケンス制御部101は、被制御機器2の状態とユーザーから要求された制御内容とにより、コマンドの送出の必要性とコマンド送出の有効性を判断する。例えば、ユーザーの要求した制御内容が、被制御機器2の状態を現在の状態にする要求である場合、コマンド送出の必要性ないと判断する（具体的な例をあげると、ユーザーから被制御機器2の電源OFFが要求された場合、被制御機器2の現状態が電源OFFの状態であればコマンドシーケンス制御部101はコマンド送出の必要がないと判断する）。このようにコマンドシーケンス制御部101が機器状態判断部103から被制御機器2の現状態情報を取得し、コマンド送出の必要性を判断することにより、電源のON/OFFのように同一コマンドによって機器の状態を順に変化させるコマンドでも被制御機器に適切に送信することが可能となる。

【0060】また、ユーザーの要求した制御内容が、被制御機器2の現状態では受け付けられない要求である場合、コマンドシーケンス制御部101がコマンド送出が無効と判断する。（具体的な例をあげると、被制御機器がTVの場合、TVの現状態が電源OFFである時にユーザーからチャンネル変更の要求を受信した場合、TVの現状態が電源ON以外ではチャンネル変更のコマンドはTVに受け付けられないため、コマンド送出が無効と判断する）。

【0061】このようにコマンドシーケンス制御部101がコマンド送出の有効性を判断することにより、被制御機器2が無視するリモコン信号を無駄に送信することがなくなる。また、被制御機器2のリモコン信号受信部が障害物等によりリモコン信号が受信できなくなっている障害状態と、被制御機器2に無視するリモコン信号を送出している操作ミスの状態とを区別することが可能となる（S9A3）。コマンド送出の必要ないと判断された場合、ユーザI/F部100を通じてユーザーに応答が返され処理が終了する（S9A7）。

【0062】コマンド送出の必要があると判断された場合、まず、コマンドシーケンス制御部101は、機器情報管理部102が管理する登録機器情報表を参照し、ユーザーが制御を要求した被制御機器2の被制御機器種別と被制御機器に対してリモコン信号を送出することが可能なコマンド送出部104を特定する。そして、被制御機器種別を用いて、機器情報管理部102が管理する機器情報表、送信フォーマット表を参照し、ユーザーが要求した制御を行うためのリモコン信号の送信フォーマットとコマンドコードを得る（S9A4）。

【0063】ユーザー要求に対応する被制御機器2の送信フォーマットとコマンドコードを得たコマンドシーケンス制御部は、通信部106を通じて被制御機器2に対応するコマンド送出部104にコマンド送出を指示する。コマンド送出の指示を受けたコマンド送出部104は、

指示された送信フォーマットで指示されたコマンドコードのリモコン信号を送出する。送出されたリモコン信号は、被制御機器2に受信されコマンドコードに従って各機器の処理が実行される(S 9 A 5)。

【0064】コマンド送出部104を通じて被制御機器2にリモコン信号を送信後、コマンドシーケンス制御部101は、機器状態判断部103にリモコン信号を送出した被制御機器2の状態を問い合わせる。被制御機器2の状態を受け取ったコマンドシーケンス制御部は、被制御機器2がリモコン信号受信し、ユーザが要求した状態に遷移しているかをチェックする(S 9 A 6)。状態が遷移している場合、ユーザI/F部100を通じてユーザに応答が返され処理が終了する(S 9 A 7)。

【0065】被制御機器2の状態がユーザの要求に合致する状態に遷移していない場合、コマンドシーケンス制御部101は、リトライ回数をチェックしリトライを行うかを判断する(S 9 A 8)。リトライ回数が予め定められた閾値N以下の場合、リトライ回数をインクリメントし、再度、リモコン信号の送出処理(S 9 A 4)を起動させる(S 9 A 10)。

【0066】このように、コマンド送出後に被制御機器2の状態をチェックしリトライ処理を行うことにより、被制御機器2の制御成功率を向上させることができるとなる。例えば、現状の機器は、赤外線によりリモコン信号を伝達するため、コマンド送出部104が被制御機器2にリモコン信号を送信した時に、被制御機器2のリモコン受信部の前に人等の障害物がたまたま存在した場合、リモコン信号は被制御機器2に制御に受信されない。そのため、結果として機器の制御が失敗することになる。リモコン信号送出後に被制御機器の状態をチェックし、リトライを行うと、被制御機器の前の障害物がなくなるとリモコン信号が正常に受信され、被制御機器の制御を成功させることができる。このようにリトライ処理を行うことが、被制御機器2の制御成功率を向上させることにつながる。

【0067】一方、リトライ回数が予め定められた閾値Nを超えている場合、コマンドシーケンス制御部101はリトライを行わず、ユーザI/F部100を通じて機器制御に失敗した旨の障害通知を行う(S 9 A 9)。被制御機器の状態をチェックし、リトライを行っても意図した状態に遷移しない場合、機器制御に失敗した旨の障害通知をユーザに送ることにより、ユーザが、同様の機能を持つ被制御機器が他にある場合、他の被制御機器を操作して目的を達する等の代替処理を行うことが可能となる。

【0068】次に、タイマー処理が行われた場合について説明する。タイマー処理の場合には、前述したコマンド送出シーケンスの処理に加えて、予約された時刻になった時に実行する処理が必要になる。まず、このコマンドシーケンス制御部101が行うタイマー処理の必要性につ

いて、例を挙げて説明する。例えば、今、電源がOFFになっているビデオにタイマー録画予約を行う場合を考えると、次の制御を順に行うことになる。  
①電源をONする。  
②録画を行う日付、時間、チャンネル等の予約情報をセットする。  
③電源をOFFにする。

【0069】ここで、現行の家庭用ビデオを想定して考えると、ビデオは赤外線によるリモコン信号を受信し処理を実行するだけで、リモコン信号を正常に受信したか、処理が成功したか等の自身の状態を返すインターフェースを備えていない。そのため、本実施の形態ではビデオ(被制御機器)にコンセント型や光センサー型の機器情報収集部を取り付け、ビデオ(被制御機器)の動作によって生じる現象(消費電力、ビデオの表示部の状況等)を収集し、機器状態判断部103が機器の状態を推測する。このことで、ビデオ(被制御機器)がリモコン信号を正常に受信したか、リモコン信号で要求した処理が成功したかを判断可能としている。

【0070】しかし、機器情報収集部が収集できる情報は限られているため、ビデオの内部状態だけを変化させ、ビデオの外部にその変化が現象として現れないものに関しては検出することができない。このビデオの例では、「②録画を行う日付等の予約情報をセットする」のステップが、機器状態収集部105で十分に情報を収集できない場合に相当する。なぜなら、「②録画を行う日付等の予約情報をセットする」のステップに関するリモコン信号を受信し、その処理に成功しても失敗してもビデオの内部状態だけが変化し、ビデオの消費電力や表示部の表示が変化しないためである。タイマー録画予約の場合、「②録画を行う日付等の予約情報をセットする」のステップが成功していたかを知る情報を機器情報収集部が検出できるのは、タイマーをセットした時間になり、ビデオの電源がONになって録画等が始まった時である。ここでは、ビデオの予約録画を例に説明したが、エアコンのタイマー予約やTVのタイマー予約等でも同様である。

【0071】このタイマー予約に関する問題を解決するため、コマンドシーケンス制御部はタイマーを予約した時間に被制御機器2の状態をチェックするシーケンスを実行する。コマンドシーケンス制御部がタイマーを予約した時間に実行する処理のシーケンスを図28に示す。

【0072】ユーザI/F部100を通じて、ユーザから被制御機器2に関するタイマー予約処理が要求された場合、コマンドシーケンス制御部101は、前述の図9のシーケンスに従いタイマー予約に関するリモコン信号を被制御機器2に対して送出する。そして、コマンドシーケンス制御部101は、タイマー予約を行った機器とその予約内容を記憶し処理を一旦完了する。その後、タイマー予約を行った時間になると、コマンドシーケンス制御部101は、タイマー予約を行った被制御機器2の状態をチェックし、必要に応じてコマンド送信処理を実

行する。

【0073】図28を参照しながら、タイマー予約時間にコマンドシーケンス制御部101が行う処理について詳細を説明する。タイマー予約時間になると処理がスタートし(S9B1)、まず、リトライ回数が初期化される(S9B2)。次に、コマンドシーケンス制御部101が機器状態判断部103に被制御機器2の状態を問い合わせ、目的の状態に被制御機器の状態が遷移しているかを確認する。目的の状態に遷移している場合、タイマー予約に関する処理を終了する(S9B3)。

【0074】一方、目的の状態に遷移していない場合、コマンドシーケンス制御部101は、被制御機器2の状態を遷移させるためのリモコン信号を前述の図9のコマンド送出シーケンスの場合と同様に、送信フォーマット表及び機器情報表から得る(S9B4)。

【0075】そして、コマンド送出部104から被制御機器2へリモコン信号を送出させる(S9B5)。その後、再度、機器状態判断部103から被制御機器2の状態を得て、被制御機器2が目的の状態に遷移しているかを検証する。目的の状態に遷移している場合、タイマー予約に関する処理を終了する(S9B6)。

【0076】目的の状態に遷移していない場合、まず、リトライ回数をチェックする(S9B7)。リトライ回数が予め定められた閾値Nを超えている場合、ユーザI/Fを通じてコマンドシーケンス制御部101はリトライを行わず、ユーザI/F部100を通じてタイマー処理が動作していない旨の障害通知を行う(S9B8)。障害通知をユーザに送ることにより、ユーザが、同様の機能を持つ被制御機器が他にある場合、他の被制御機器を操作して目的を達する等の代替処理を行うことが可能となる。

【0077】リトライ回数が予め定められた閾値N以下の場合は、コマンドシーケンス制御部101は、リトライ回数をインクリメントし、再度、コマンド送出部104から被制御機器2へリモコン信号の送信を行うようにさせる(S9B9)。そして、その後、再度、被制御機器の状態をチェックするリトライ処理を行う。このようにリトライ処理を行うことが、被制御機器2の制御成功率を向上させることにつながる。

【0078】具体的に前述のビデオの例を用いてタイマー予約の録画開始予約を行った時間にコマンドシーケンス制御部101が行う制御を説明する。まず、コマンドシーケンス制御部101は、ビデオの状態が録画状態になっているかをチェックする。録画状態になっている場合、以前に実行した録画予約処理が正常に行われていたと判断し、処理を終了する。一方、録画状態にならない場合、録画予約処理が正常に実行されなかったと判断し、録画予約処理の再実行をするのではなく直接録画処理を起動させるために以下のリモコン信号送出処理を実行する。  
①ビデオの電源を入れる。  
②ビデオのチャン

ネルを切り替える。  
③録画を開始させる。この処理によって、録画予約に失敗していたとしてもユーザが要求した番組の録画が正常に行われることになる。この時、前述した通り各リモコン信号送出後に被制御機器の状態がチェックされ、目的の状態に遷移していない場合、リトライ回数がチェックされた上でリトライ処理が実行される。

【0079】また、「②ビデオチャネルを切り替える」のリモコン信号のように、被制御機器が複数回同じ信号を受信しても誤動作につながらないリモコン信号の場合、コマンド送出部が、リモコン信号送出時に同じ信号を複数回送出することで、被制御機器の制御の確実性を向上させることが可能となる。なお、「①ビデオの電源を入れる」は、被制御機器の状態をチェックした上で必要に応じて行う（ビデオが電源ON状態になっている場合には行わない）。

【0080】さらに、タイマー予約の録画終了予約を行った時間に、先の制御と同様にコマンドシーケンス制御部101が録画の終了を制御するための処理を起動する。まず、コマンドシーケンス制御部101は、ビデオの状態が電源オフの状態になっているかをチェックする。電源オフの状態になっている場合、録画終了処理が正常に行われたと判断し終了する。一方、電源オフの状態にならない場合、コマンドシーケンス制御部101が電源オフの状態にするためのリモコン信号を送出させる。そして、被制御機器（ビデオ）の状態をチェックし、目的の状態に遷移していない場合、リトライ回数がチェックされた上で、再度リモコン信号送出処理が実行される。

【0081】次に、機器状態判断部103が機器情報収集部105から得た情報をもとに被制御機器2の状態を判断する処理の詳細について述べる。まず、機器状態判断部103は、状態を判断したい被制御機器2に接続されている機器情報収集部105を特定する。機器情報収集部105の特定は、登録機器情報表を用いて行われる。登録機器情報表から機器情報収集部を特定する情報（機器情報収集部ID）を取得した機器状態判断部103は、通信部106を通じて該当する機器情報収集部105にアクセスし、状態を判定したい被制御機器2の動作によって生じた現象の情報を得る。得た現象の情報と機器情報管理部102が管理する機器情報表の状態解析用情報とから各被制御機器2の状態を判断する。

【0082】さらに、機器情報収集部105が収集する被制御機器2の動作によって生じる現象情報と機器情報表の状態解析用情報との関係について、具体例を挙げてより詳細に説明する。図6は、被制御機器の1つであるビデオの各状態と消費電力の関係を示している。ビデオは電源OFFの状態では、リモコン信号を受け付けるため等に若干電力を消費している。電源ONの状態では、チューナ部等が電力を消費するため電源OFFの場合よ

り消費電力が高くなる。そして、録画状態では、チューナ部等に加えてテープ走行系などの機構系の消費電力が加わるため電源ONの場合よりさらに消費電力が高くなる。このように、消費電力を計測すると被制御機器2の状態をある程度推測する事が可能となる。この被制御機器2の消費電力を計測する目的で用いられるのが図4に示したコンセント型の機器情報収集部である。また、被制御機器の状態と消費電力の関係は、機器情報管理部が管理する機器情報表の状態解析用情報に記載されている。

【0083】しかし、消費電力だけで全ての状態が判断できない場合も存在する。例えば、ビデオの場合には、再生中状態と録画中状態が消費電力だけでは区別できない場合がある。このような場合、別の測定機能を持つ機器情報収集部105を併用したり、別の測定機能を持つ機器情報収集部105を用いたりする。図5は、光センサー型の機器情報収集部とビデオへの取り付けの一例を示している。

【0084】図7は図5のように光センサー型の機器情報収集部をビデオに取り付けた場合の光センサーに流れる電流とビデオの状態を示している。ビデオは、再生が始まると表示部の再生中を示すLEDが点灯する。また、録画を開始した場合、録画中を示す表示部のLEDが点灯する。このLEDの光を光センサーが感知することによって、録画中、再生中ににおいて、対応する光センサー(A)、(B)の電流量が増加する。この光センサーの反応により、ビデオの録画中状態と再生中状態をも識別することが可能となる。(これに加えて、電源ランプにも光センサーを取り付ければ、電源のON、OFFも識別可能となる) このLEDの点灯を光センサーを用いて計測するのが光センサー型機器情報収集部である。光センサー型機器情報収集部105が収集する情報と各被制御機器2の状態との対応は、機器情報管理部が管理する機器情報表の状態解析用情報に記載されている。

【0085】なお、本実施の形態では機器情報収集部105として、コンセント型と光センサー型のみを説明したが、クーラーやストーブでは温度センサーや風力センサー、洗濯機等では振動センサーや加速度センサーを用いて、光センサー型やコンセント型と同様に被制御機器の状態を推測できる。

【0086】次にアイロン、こたつ、蛍光灯等のリモコン信号を受信する機能を有していない被制御機器を機器制御システムで制御する場合について説明する。リモコン信号を受信する機能を有していない被制御機器を機器制御システムに収容する場合は、必ずコンセント型機器情報収集部を接続する。コンセント型機器情報収集部は、被制御機器2の電源プラグと電源コンセントとの間に接続され、被制御機器2の消費電力(電流)量の測定機能に加えて、コマンドシーケンス制御部からの指示により被制御機器2への電力供給のON・OFFを制御する

機能を有する。コンセント型機器情報収集部2より、前記したビデオ等の場合と同様に被制御機器の状態を知ることが可能となる。また、コンセント型機器情報収集部2が持つ被制御機器への電力供給制御機能を用いることにより、コマンドシーケンス制御部は被制御機器の電源ON・OFFの制御を行うことが可能となる。

【0087】なお、現状の機器ではリモコン信号として赤外線が使用されている。そのため、被制御機器のリモコン受信部に障害物があると被制御機器はリモコン信号を受信することができなくなる。ゆえに、その障害物がどれられなければ、被制御機器は制御不能となる場合がある。一方、機器情報収集部105とコマンドシーケンス制御部101との通信は、無線や電力線等を通じて行うことで障害物等の影響を受けなくすることが可能である。そこで、リモコン信号受信機能を持つ機器(例えば、テレビ、ビデオ等)にも電力供給のON・OFFを制御する機能を持つコンセント型機器情報収集部2を用いることにより、制御不能となった被制御機器2への電力供給を強制的にONすることができる。

【0088】以上のように、本発明によれば、機器情報収集部105が被制御機器2の動作によって生じた現象の情報を収集し、機器状態判断部103が収集した情報から各被制御機器2の状態を推測することにより、従来家電(リモコン信号の受信機能しかもたない機器又は、リモコン信号の受信機能すら持たない機器)の状態を遠隔から知ることが可能となる。

【0089】また、コマンドシーケンス制御部101が、機器状態判断部103より各被制御機器2の状態を参照しながらリモコン信号の送出を指示することにより信頼性の高い遠隔制御が可能となる。

【0090】(実施の形態2)以下、本発明の実施の形態2について図面を参照しながら説明する。図11は本発明の実施の形態2における機器制御システムの一構成例である。なお、実施の形態1と同様の機能部については、同一の符号をつけ説明を省略する。

【0091】図11において、10はユーザ1/F部100とコマンドシーケンス制御部101と機器情報管理部102と機器情報判断部103と通信部106から構成され、機器制御システム全体の制御を行う制御親機部、11はコマンド送信部と機器登録受付部108と通信部106とで構成され、被制御機器の登録受付及び被制御機器への制御信号送信を行う制御子機部、108は被制御機器の機器制御システムへの新規登録と機器情報収集部105の機器制御システムへの新規登録を受け付ける機器登録受付部である。機器情報収集部105は、制御親機部の通信部106を通じて機器状態判断部103及びコマンドシーケンス制御部101との通信を行う。また、機器登録受付部108及びコマンド送信部104は、制御子機部11と制御親機部10の通信部106を通じて、機器状態判断部103、コマンドシーケン

ス制御部 101、機器情報管理部 102 と通信を行う。  
【0092】図12は実施の形態2での制御親機部100、制御子機部11、機器情報収集部105の配置の一例を示している。制御子機部11のコマンド送出部104は、赤外線によるリモコン信号を送出する機能部であり、部屋内の被制御機器2を見通せる位置に配置することで、複数の被制御機器2に対してリモコン信号を送信することが可能となる。しかし、赤外線信号は壁等の障害物を通り抜けることができないため、他の部屋の被制御機器2に対してリモコン信号を送信することはできない。また、制御子機部11の機器登録受付部108は、被制御機器2又は機器情報収集部105を機器制御システムへ新規登録する際の受付処理を行う。

【0093】機器情報収集部105と被制御機器2の機器登録受付部108への新規登録用の信号送信は赤外線信号を用いて行う。制御子機部11と制御親機部100との間の通信は、電力線、無線等を用いて行われる。機器情報収集部105と機器情報判断部103及びコマンドシーケンス制御部101との通信も同様に電力線、無線等を用いて行われる。なお、機器情報収集部105は赤外線信号で通信を行い、制御子機11が通信の中継を行うことで、機器情報収集部105と機器情報判断部103及びコマンドシーケンス制御部101との通信を可能としても良い。

【0094】図13は実施の形態2における制御子機部11の構成の一例を示している。制御子機部11は本体部に照明用コンセントに差し込むための突起部と、照明の電源プラグを接続するための差込口を持ち、本体部に接続された支持部上に赤外線信号の発生と赤外線信号の受信を行う赤外線送受信素子が取り付けられている。赤外線送受信素子は、コマンド送出部104と機器登録受付部108に接続されており、コマンド送出部からの信号により、赤外線送受信素子は赤外線を発射する。また、赤外線送受信素子は赤外線を受信した場合、受信した信号を機器登録受付部108に送信する。

【0095】このように制御子機部に照明用コンセントに差し込むための突起部と、照明の電源プラグを接続するための差込口を設けることにより、照明用コンセントは一般に部屋の中央の天井に設けられるため、部屋内にある各被制御機器2を見通しが利く天井中央に制御子機部11を取り付けることが可能となり、且つ、照明器具により照明器具により制御子機部11が隠されるため美観を損ねることがないというメリットが生じる。さらに、赤外線送受信素子を支持部に取り付けることにより、制御子機部に接続された照明器具によって制御子機が発射する赤外線リモコン信号が遮られるのを防ぐことと、新規被制御機器登録時に送られてくる赤外線信号が遮られるのを防ぐことができる。

【0096】以上のように構成されたリモートコントロールシステムについて、以下その動作を説明する。ユー

ザが被制御機器2の現状態の問い合わせを行った場合の処理、ユーザが被制御機器2の制御を要求した場合の処理、タイマー予約が行われた場合の処理については、実施の形態1と同様であり、説明を省略する。

【0097】実施の形態2の特徴は、被制御機器2の登録処理にある。実施の形態1では、図2の登録機器情報表は、ユーザがユーザI/Fを通じて、機器制御システムで制御する被制御機器に関する情報を全て入力することで作成されていた。実施の形態2の機器登録方法は、この手順を簡略化し、ユーザの利便性を高めるものである。新規被制御機器2を機器制御システムに登録する処理シーケンスを図14に示す。以下、図14の新規被制御機器2の登録シーケンスについて説明する。

【0098】被制御機器2を新たに機器制御システムに登録する場合、ユーザがユーザI/F部を通じて、新規被制御機器を登録する旨をシステムに通知する。この時、ユーザは、新規登録を行いたい被制御機器が赤外線によるリモコン制御が可能な機器か、又は、リモコン制御ができない機器を示す情報を添付する。新規登録の通知を受けたユーザI/F部100は、ユーザから受け取った情報を機器情報管理部102に通知する(S141)。通知を受けた機器情報管理部102は機器登録モードに状態を遷移させ、新規に登録しようとしている被制御機器が赤外線によるリモコン制御が可能かどうかをチェックする(S142)。

【0099】新規登録したい被制御機器2が赤外線によるリモコン制御が可能である場合、機器登録受付部108からの機器登録情報を待つ。新規被制御機器の登録を行うユーザは、新規に登録したい被制御機器2のリモコンを用いて、制御子機部11の機器登録受付部に向けて電源ON/OFF用の赤外線リモコン信号を送信する。赤外線リモコン信号を受信した機器登録受付部108は、受信したリモコン信号と自分が属する制御子機部11のIDを含んだ機器登録情報を通信部106を通じて機器情報管理部102に送信する(S146)。

【0100】機器登録情報を受信した機器情報管理部102は、機器登録情報よりリモコン信号を取り出し、送信フォーマット表、機器情報表を用いて、新規に登録する被制御機器の機器種別の絞り込みを行う。リモコン信号は、機器の製造メーカーにより送信フォーマットが異なり、同じ製造メーカーでも機器の種類(例えば、TVとビデオ等)によって制御用コマンドコードが異なる。ゆえに、電源ON/OFF用の赤外線リモコン信号を解析すると、機器の製造メーカーと機器の種類を特定することが可能となる。

【0101】機器種別の絞り込みを実行した結果、被制御機器2の機器種別として複数の候補が残った場合には、ユーザI/Fを通じて被制御機器2の機器種別の候補をユーザに提示し、ユーザに被制御機器2の機器種別を選択させる。機器種別の特定が完了した機器情報管理

部102は、登録機器情報表へ新規被制御機器の登録処理を実行する。制御子機部IDから変換する部屋名（1F和室、1F居間等）と機器種別から変換する機器名（ビデオ、テレビ等）を用いて被制御機器名を登録する。そして、被制御機器種別と、制御子機部IDからコマンド送出部IDを特定してコマンド送出部IDを登録する（S147）。

【0102】機器登録受付部108からの機器登録情報に関する登録を完了した機器情報管理部102は、機器情報収集部105からの新規登録要求の受信を持つ。機器情報収集部105の新規登録は、機器情報収集部105に設けられた新規登録用ボタンをユーザが押すことによって実行される。新規登録用ボタンが押されると、機器情報収集部105は、自らの機器情報収集部IDを含む新規登録要求を機器情報管理部102に送信する（S148）。機器情報収集部105からの新規登録要求を受信した機器情報管理部102は、新規登録要求から機器情報収集部IDを取り出し、現在新規被制御機器の登録を実行中のエン通りに登録する（S149）。

【0103】機器情報収集部105の登録を完了した機器情報管理部102は、状態を遷移させ機器登録受付モードを解除する（S1410）。このように、新規登録を行う被制御機器2がリモコン制御が可能である場合、被制御機器2のリモコンを用いて機器登録受付部に赤外線リモコン信号を送り機器登録情報を作成させることにより、登録機器情報表への情報登録処理が自動化できる。

【0104】次に、新規登録したい被制御機器2が赤外線によるリモコン制御ができない機器である場合を説明する。機器情報管理部102は、機器情報収集部105からの新規登録要求の受信を持つ（S143）。ユーザにより機器情報収集部105に設けられた新規登録用ボタンが押され、機器情報収集部105が送信した機器情報収集部IDを含む新規登録要求を機器情報管理部102が受信すると、機器情報管理部102は新規登録要求より機器情報収集部IDを取り出し、機器登録表に新たに登録する（S144）。

【0105】機器情報収集部105からの新規登録要求だけでは、被制御機器名情報、被制御機器種別等の情報が不足しているため、ユーザI/F部を通じてユーザからの情報入力を要求する。ユーザから被制御機器名情報、被制御機器種別等の情報が入力されると、機器情報管理部102は機器情報表に登録する（S145）。そして、機器情報収集部105の登録を完了した機器情報管理部102は、状態を遷移させ機器登録受付モードを解除する（S1410）。機器登録受付モードが解除されている状態で、機器情報収集部105からの新規登録要求や機器登録受付部108からの機器登録情報を受信した場合、それらの情報は無視される。このことによつて、ユーザが誤って新規登録動作を行った場合の誤動作

が防止される。

【0106】なお、1つの被制御機器2に対して複数の機器情報収集部105を登録する場合、ユーザがユーザが当初に複数の機器情報収集部105を登録することを通知しておき、機器情報収集部105の登録手順が複数回行われる。

【0107】次に、被制御機器2の登録削除シーケンスについて説明する。登録削除は図15に示すシーケンスで実行される。被制御機器2を機器制御システムから削除する場合、ユーザはユーザI/F部100を通じて、登録機器削除したい旨をシステムに通知する。登録機器削除の通知は機器情報管理部102に送られる。登録機器削除の通知を受けた機器情報管理部102は、ユーザI/F部100を通じて、登録機器情報表に登録されている被制御機器2の一覧を示し、削除したい被制御機器2をユーザに選択させる（S151）。ユーザが削除したい被制御機器2を選択すると、その情報が機器情報管理部102に通知される。通知を受けた機器情報管理部102は、登録機器情報表の対応するエン通りを削除する（S152）。

【0108】以上のように本実施の形態によれば、制御子機部に照明用コンセントに差し込むための突起部と、照明の電源プラグを接続するための差込口を設けることにより、照明用コンセントは一般に部屋の中央の天井に設けられるため、部屋内にある各被制御機器2を見通しが利く天井中央に制御子機部11を取り付けることが可能となり、且つ、照明器具により照明器具により制御子機部11が隠されるため美観を損ねることがないというメリットが生じる。さらに、赤外線送受信素子を支持部に取り付けることにより、制御子機部に接続された照明器具によって制御子機が発射する赤外線リモコン信号が遮られるのを防ぐことと、新規被制御機器登録時に送られてくる赤外線信号が遮られるのを防ぐことができる。

【0109】また、機器制御システムに新たな被制御機器2を登録する時、機器登録受付部108に対して被制御機器2用のリモコンが送出するリモコン信号を入力する。そして、機器情報管理部102がそのリモコン信号を機器登録受付部108から受け取り、解析し被制御機器2の情報を登録機器情報表に設定し、同時に機器登録受付部108が属する制御子機に内蔵されたコマンド送出部104のIDを登録機器情報表に設定することにより、被制御機器の登録手順を簡単化することができる。

【0110】（実施の形態3）図16は本発明の実施の形態3における宅外から制御可能な機器制御システムの構成を示すものである。図16において、20aはインターネット21を介して宅外から機器制御システムにアクセスし、被制御機器2を制御可能なユーザ端末、20bは電話網22を介して宅外から機器制御システムにアクセスするユーザ端末、21はインターネット、22は回線交換で通信を可能とする電話網、201は通信情報

解析部 203 が指示する通信条件に従いながら、インターネット 21 を通じてユーザ端末 21 との通信を制御するインターネットアクセス部、202 は電話網 22 を通じた通信を制御し、通信条件解析部 203 に通信情報

(発電話番号、端末番号、位置情報等) を提供する電話網アクセス部、203 は電話網アクセス部から通信情報(発電話番号、端末番号、位置情報等)を得て、その通信情報によりユーザ認証を行い、認証結果に応じてインターネットアクセス部の通信条件を設定する通信情報解析部、204 は被制御機器 2 への制御コマンドを送信等、被制御機器の制御を行う機器制御部、2 はコンピュータ、AV 機器、家電等の被制御機器である。

【0111】以上のように構成された機器制御システムについて、以下、図 17 から図 27 を用いてその動作を説明する。図 17 は機器制御システムが常時接続の形態でインターネットに接続されている場合におけるインターネットを通じたアクセスの開始シーケンスを示している。

【0112】宅外のユーザは、まず、電話網 22 を通じてアクセスするユーザ端末 20b (電話機) を用いて、機器制御システムの電話網アクセス部へ発呼する。そして、電話網アクセス部が着呼を検出する (S171)。電話網 22 より着呼を検出した電話網アクセス部 202 は、ユーザ端末 20b (電話機) の発番号 (発呼元電話番号) を電話網 22 より入手する。入手したユーザ端末 20b の発番号を通信情報解析部 203 に通知する (S172)。

【0113】通信情報解析部 203 は、通知された発番号が通信解析部 203 が管理する認証情報表に登録されているかをチェックする。認証情報表に通知された発番号が登録されていない場合、処理を終了する。また、認証情報表に通知された発番号が登録されている場合、S174 の処理を実行する (S173)。ここで、認証情報表は、機器制御システムに宅外からのアクセスを許諾するユーザの情報を管理するものであり、この実施の形態では図 18 のようにユーザが宅外からのアクセスを使用する電話機の発番号と IP アドレス対応が記載されている。

【0114】認証情報表に通知された発番号が登録されている場合、認証情報表から対応する IP アドレス (ユーザ端末 20a の IP アドレス)を取り出し、インターネットアクセス部 201 のパケットフィルタリングの設定を変更して、ユーザ端末 20a が通信先となる IP パケットを通すようにさせる (S174)。なお、インターネットアクセス部の初期状態は、全ての外部からの IP パケットが通らないように設定されている。このことによって、外部から一切 (不正) アクセスができなくなっている。また、パケットフィルタリングの設定変更を初期状態に戻す制御については後述する。

【0115】インターネットアクセス部 201 のパケッ

トフィルタリングの設定がユーザ端末 20a の IP アドレスを通すように設定変更された後、ユーザはユーザ端末 20a (PC) でインターネット 21 を通じて、機器制御システムにアクセスすることが可能となる。具体的には、ユーザ端末 20a (PC) から機器制御用の情報を入力した IP パケットを送信すると、インターネット 21 を通じて、インターネットアクセス部に到着する。

【0116】インターネットアクセス部のパケットフィルタリングは、許可された送信元からの IP パケットであるため、機器制御部 204 に情報を引き渡す。機器制御部 204 は受信した情報により機器の制御を実行する。但し、インターネットアクセス部がユーザ端末 20a と通信を開始する際には、一般的のコンピュータ機器で使用されているユーザ名とパスワードを用いたログイン処理を実行させる。なお、許可されない IP パケットであった場合には、インターネットアクセス部 201 がパケットを廃棄する。

【0117】次に、電話網アクセス部 202 への着呼検出によって変更されたインターネットアクセス部の設定を初期状態に戻す制御について記述する。図 19 はインターネットアクセス部の設定をリセットする処理について記述している。

【0118】通信情報解析部 203 が、ユーザ端末 20a の IP アドレスに関してインターネットアクセス部 201 のパケットフィルタリングの設定を変更すると、インターネットアクセス部で通信条件のリセット用処理が起動する (S191)。ユーザ端末 20a が機器制御システムへのアクセス終了時に送信するメッセージの受信 (例えば、ログアウトメッセージの受信が相当する) を監視する (S192)。

【0119】アクセス終了メッセージを受信した場合、インターネットアクセス手段がユーザ端末 20a の IP アドレスに関するパケットフィルタリングの設定をリセットする。これにより、以後、ユーザ端末 20a から機器制御システムへのアクセスが不可能になる。ユーザ端末 20a から再度アクセスする場合には、再度、ユーザ端末 20b を用いて機器制御システムに発呼する必要がある (S194)。

【0120】アクセス終了メッセージを受信していない場合、インターネットアクセス部の通信条件 (パケットフィルタリングの設定) を変更してからの時間が、予め定められた時間 T 以上経過していないかをチェックする。T 時間以上経過している場合には、S194 の通信条件のリセット処理を起動する。また、T 時間未満しか経過していない場合には、再び、S192 の終了メッセージ監視を行う (S193)。

【0121】以上のように、通信情報解析部 203 が、電話網アクセス部 202 から得た通信先情報 (発呼元電話番号) の認証を行い、認証に合格した場合にのみインターネットアクセス部 201 の設定を変更し宅外からの

インターネットを通じたアクセスを可能とすることにより、機器制御システムに不正アクセスするためには電話網にも不正アクセスする必要があるため、インターネットを通じた機器制御システムへの不正アクセスを非常に困難にすることができる。

【0122】また、通信情報解析部203がインターネットアクセス部201の通信条件（パケットフィルタリング条件）を変更後、予め定められた時間T以上経過した場合及び、ユーザ端末20aが機器制御システムへアクセス終了を通知した場合に通信条件をリセットすることにより、正当なユーザ端末20aのアクセス終了後には宅外からのインターネットを通じたアクセスが不可能となるため、機器制御システムへの不正アクセスを防ぐことが可能となる。

【0123】図20は機器制御システムがダイヤルアップの形態でインターネットに接続されている場合のアクセス開始シーケンスを示している。宅外のユーザは、まず、電話網22を通じてアクセスするユーザ端末20b（電話機）を用いて、機器制御システムの電話網アクセス部へ発呼する（S201）。電話網22より着呼を検出した電話網アクセス部202は、ユーザ端末20b（電話機）の発番号（発呼元電話番号）を電話網22より入手する。入手したユーザ端末20bの発番号を通信情報解析部203に通知する（S202）。

【0124】通信情報解析部203は、通知された発番号が通信解析部203が管理する認証情報表に登録されているかをチェックする。認証情報表に通知された発番号が登録されていない場合、処理を終了する。また、認証情報表に通知された発番号が登録されている場合、S204の処理を実行する（S203）。ここで、認証情報表は、機器制御システムに宅外からのアクセスを許諾するユーザの情報を管理するものであり、この実施の形態では図21のようにユーザが宅外からのアクセスに使用する電話機の発番号とIPアドレスとユーザのメールアドレスの対応が記載されている。

【0125】認証情報表に通知された発番号が登録されている場合、認証情報表から対応するIPアドレス（ユーザ端末20aのIPアドレス）を取り出し、インターネットアクセス部201のパケットフィルタリングの設定を変更して、ユーザ端末20aが通信先となるIPパケットを通すようにさせる（S204）。

【0126】通信情報解析部203がインターネットアクセス部201にダイヤルアップ接続実行の指示を行い、インターネットアクセス部201がダイヤルアップによりインターネットに接続される（S205）。通信情報解析部203がダイヤルアップによりインターネットアクセス部201に割り当てられたIPアドレスをインターネットアクセス部201を取得し、認証情報表からユーザ端末20bの発番号に対応するメールアドレスへインターネットアクセス部から取得した機器制御シ

ステムのIPアドレス情報を送信する（S206）。また、インターネットアクセス部の設定を初期状態に戻す制御については、先の常時接続の場合と基本的に同じである。但し、ダイアルアップ接続時には、S194の処理でインターネットへの接続を切る処理も行う点だけが異なる。

【0127】以上のように、通信情報解析部203が、電話網アクセス部202から得た通信先情報（発呼元電話番号）の認証を行い、認証に合格した場合にのみインターネットアクセス部201がダイヤルアップでインターネットに接続することにより、常時接続ではない形態でも宅外からインターネットを介して機器制御システムにアクセスすることが可能となる。加えて、必要ないときにはインターネットに接続されていないため、インターネットを通じた機器制御システムへの不正アクセスを防ぐことができる。

【0128】また、インターネットアクセス部201がダイヤルアップでインターネットに接続後、通信情報解析部204が機器制御システムに割り当てられたIPアドレスをユーザに通知することにより、機器制御システムがインターネット接続時にDHCP等によりIPアドレスを随時割り当てる方が用いられる場合でも、ユーザが機器制御システムのIPアドレスを知ることができ、宅外から機器制御システムにインターネットを通じてアクセスすることが可能となる。

【0129】なお、前記説明では機器制御システムのIPアドレスを電子メールでユーザに通知するとしたが、電子メールは効果的な1つの例であり、IPアドレスの通知方法としては、電話網22を通じて着呼したユーザ端末20bに通知する方法や、予め定められたURLにIPアドレスを示す情報を入ったhtmlファイルをアップロードする方法や、予め登録してあるページ等の機器に通知する方法等が考えられる。

【0130】図26は機器制御システムが常時接続の形態でインターネットに接続されている場合のアクセス開始シーケンスの第2の例を示している。宅外のユーザは、まず、ユーザ端末20aを用い、インターネット21を通じて機器制御システムへログイン要求を送る（S261）。ログイン要求を受けたインターネットアクセス部201はログイン処理を保留し、通信情報解析部203にログイン要求受信を通知する。通知を受けた通信情報解析部203は、インターネットアクセス部を通じてユーザ端末20aに乱数により発生させたチェック用情報を送信する。この時、保留させたログイン要求とチェック情報の対応関係を記憶しておく（S262）。

【0131】チェック用情報を受け取ったユーザは、ユーザ端末20bを用い、電話網22を通じて機器制御システムへ発呼する。電話網22より着呼した電話網アクセス部202は、電話網22から発呼元であるユーザ端末20bの発番号と、ユーザ端末20bからチェック用

情報を得る。ここで、チェック用情報の送信方法としては、トーン音を用いる方法、呼制御メッセージに付加させる（例えば、SETUPメッセージのユーザ・ユーザ情報を使用）方法等が考えられる（S263）。

【0132】通信情報解析部203は、通知された発番号が通信情報解析部203が管理する図27に示す認証情報表に登録されているかをチェックする。発番号が登録されている場合、チェック用情報に対応するログイン要求があるかを確認する。チェック用情報に対応するログイン要求が確認できた場合には、S265のログイン保留解除処理を起動させる。発番号が登録されていないか、又は、チェック用情報に対応するログイン要求が存在しない場合には処理を終了する（S264）。

【0133】通信情報解析部203がインターネットアクセス部201の通信条件を変更し、ログインの保留を解除し、ログイン処理を続行させる（S265）。以下、機器制御システムのログイン処理が完了すると、ユーザ端末20aはインターネット21を通じて機器制御部204と通信し被制御機器2を制御することが可能となる。また、インターネットアクセス部の設定を初期状態に戻す制御については、先の常時接続の場合と基本的に同じである。このように制御することによって、機器制御システムに登録されたユーザ端末20bを所有していない限り、チェック用情報を入力することができないため、インターネット21を介した機器制御システムへの不正アクセスを困難にすることができる。

【0134】図22は、図16の機器制御部204に実施の形態2の機器制御システムを適用した場合の構成例である。図19において、ユーザ端末20は、iモード電話機のようなインターネット網を通じた通信と電話網を通じた通信の両方が可能な端末である。

【0135】ユーザ端末20が電話網22を通じて機器制御システムの電話網アクセス部202に発呼後、インターネット21を通じて機器制御システムにアクセスすると、インターネットアクセス部201を通じてユーザ端末20の要求がユーザI/F部100に送信される。ユーザI/F部100がユーザ端末20の要求を受け取ると、要求に応じて実施の形態2と同様に被制御機器2の制御を実行し、応答をインターネットアクセス部201を通じてユーザ端末20に送信する。このように構成することにより、従来の家電機器をインターネットを介して、宅外から安全に操作することが可能となる。

【0136】なお、先の説明では、通信情報解析部203がユーザ端末の発番号を用いて認証情報表からIPアドレスを取り出し、インターネットアクセス部201のパケットフィルタリング機能に設定するとしていたが、通信情報解析部203が電話網アクセス部を通じて、着呼時にユーザ端末20（又は20b）からIPアドレスを取得しパケットフィルタリング機能に設定するとしても良い。ここで、IPアドレスの送信方法としては、ト

ーン音を用いる方法、呼制御メッセージに付加させる（例えば、SETUPメッセージのユーザ・ユーザ情報を使用）方法等が考えられる。

【0137】また、ユーザ端末20（又は20b）からIPアドレスを取得せず、通信情報解析部203がユーザ端末20（又は20b）の発番号を認証後、最初にインターネットアクセス部201が受信したログイン要求パケットの発信元IPアドレスを受け入れるようにパケットフィルタリング機能を設定する方法も考えられる。このように制御することにより、ユーザ端末20（又は20a）のIPアドレスがアクセス毎に変化する形態（例えば、ユーザ端末がアクセス開始時にDHCPでIPアドレスが割り当てられる形態）でも、宅外から安全に機器制御システムにアクセスさせることができるとなる。

【0138】また、先の説明では、通信情報解析部203がインターネットアクセス部201のパケットフィルタリング機能を設定するとしていたが、通信情報解析部203が図23(a)に示す認証情報表を管理し、ユーザ端末20（又は20b）の発番号を認証後、認証情報表からサービスクラス情報を取得してインターネットアクセス部201に設定する。そして、インターネットアクセス部201は、図23(b)に示すサービスクラス定義表を管理し、インターネット21を通じたユーザ端末20（又は20a）からの要求の内、サービスクラスに合致しない要求についてはこれを拒否するとして良い（ここで、インターネットアクセス部の初期状態では、全ての要求を拒否する）。このように制御することで、宅外からアクセス可能なユーザが多数いたとしても、特定のユーザ端末20bを持つユーザだけがセキュリティ上重要な処理を実行可能とできるため、宅外からの機器制御システム制御の安全性を向上させることができる。

【0139】また、通信情報解析部203が図24に示す認証情報表を管理し、ユーザ端末20（又は20b）の発番号を認証後、認証情報表からユーザ名情報とパスワード情報を取り出してインターネットアクセス部201に設定する。そして、インターネットアクセス部201は、インターネット21を通じたユーザ端末20（又は20a）が機器制御システムへログインする時にユーザ名とパスワードを要求し、前記通信情報解析部203が設定したユーザ名とパスワードと一致しなければ機器制御システムへログインさせないとしても良い（ここで、インターネットアクセス部の初期状態では、ユーザ名とパスワードが設定されていないため、どのようなログイン名でもログインすることができない）。このように制御することで、ユーザ端末20（又は20b）を持たなければログインできないことに加えて、ユーザ端末20（又は20b）とログイン名、パスワードの正しい組み合わせを知るユーザだけがログイン可能とできるため、宅外からの機器制御システム制御の安全性を向上さ

せることができる。

【0140】さらに、通信情報解析部203が図25に示す認証情報表を管理し、ユーザ端末2.0（又は20b）の発番号を認証後、複数の設定（パケットフィルタリングのIPアドレス、ユーザ名とパスワード、サービスクラス等）を行う。そして、インターネットアクセス部201は、インターネット2.1を通じたユーザ端末2.0（又は20a）が前記設定に合致しなければ、機器制御システムへのアクセスが不可能にさせる。このように、電話網2.2から通信情報を得て認証した後、複数の通信条件をインターネットアクセス部201に設定することで、宅外からの機器制御システム制御の安全性をより向上させることができることは自明である。

【0141】本実施の形態では、通信情報解析部203が設定するパケットフィルタリングの条件として宅外ユーザ端末のIPアドレスについて説明したが、当然、被制御機器がIPアドレスを持つなら被制御機器のIPアドレス、加えて、発信元、発信先のポート番号等もパケットフィルタリングの条件として設定することが安全性を向上させる上で効果的なのは自明である。

【0142】上記の制御例は、本発明の実施形態の一例であり、本発明の本質は電話網2.2から通信情報を得て認証を行い、その結果をもとにインターネットアクセス部201の設定を変更し、インターネットを介した通信を可能とさせる点にある。ゆえに、電話網2.2から通信情報（ユーザ端末2.0（又は20b）の発番号（電話番号）、端末識別番号、位置情報、通信に利用している無線基地局ID等）やインターネットアクセス部201に設定する情報の組み合わせにより、多数の制御シーケンスのバリエーションを考えることができるが、これらは全て自明である。

【0143】このような制御により、機器制御システムへインターネットを通じて不正アクセスするには、電話網2.2とインターネット2.1の両方をハッキングする必要が生じるため、不正アクセスが非常に困難となる。しかも、正当なユーザにとっては、電話をかけるという簡単な手順しか追加されないため、専門知識がないユーザでも簡単に導入することができる。

#### 【0144】

【発明の効果】以上のように、本発明によれば、機器情報収集部105が被制御機器2の動作によって生じた現象の情報を収集し、機器状態判断部103が収集した情報から各被制御機器2の状態を推測することにより、従来家電（リモコン信号の受信機能しかもない機器又は、リモコン信号の受信機能すら持たない機器）の状態を遠隔から知ることが可能となる。また、コマンドシーケンス制御部101が、機器状態判断部103より各被制御機器2の状態を参照しながらリモコン信号の送出を指示することにより信頼性の高い遠隔制御が可能となる。

【0145】さらに、機器制御システムに新たな被制御機器2を登録する時、機器登録受付部108に対して被制御機器2用のリモコンが送出するリモコン信号を入力する。そして、機器情報管理部102がそのリモコン信号を機器登録受付部108から受け取り、解析し被制御機器2の情報を登録機器情報表に設定し、同時に機器登録受付部108が属する制御子機に内蔵されたコマンド送出部104のIDを登録機器情報表に設定することにより、被制御機器の登録手順を簡素化することができる。

【0146】加えて、電話網2.2から通信情報を得て認証を行い、その結果をもとにインターネットアクセス部201の設定を変更し、インターネットを介した通信を可能とさせることにより、機器制御システムへインターネットを通じて不正アクセスするには、電話網2.2とインターネット2.1の両方をハッキングする必要が生じるため、不正アクセスが非常に困難となり、しかも、正当なユーザにとっては、電話をかけるという簡単な手順しか追加されないため、専門知識がないユーザでも簡単に導入することができるという優れた効果が得られる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態1における機器制御システムの構成図

【図2】同実施の形態における動作説明のための登録機器情報表の一例を示す図

【図3】同実施の形態における動作説明のための送信フォーマット表と機器情報表の一例を示す図

【図4】同実施の形態におけるコンセント型機器情報収集部の一例を示す図

【図5】同実施の形態における光センサー型機器情報収集部の一例を示す図

【図6】同実施の形態におけるビデオの各状態と消費電力の関係例を示す図

【図7】同実施の形態における光センサー型機器情報収集部をビデオに取り付けた場合の光センサーに流れる電流とビデオの状態例を示す図

【図8】同実施の形態におけるユーザが被制御機器2の現状態の問い合わせを行った場合のシーケンスを示す図

【図9】同実施の形態におけるユーザが被制御機器2の制御を要求した場合のシーケンスを示す図

【図10】同実施の形態における機器制御システムの家庭内配置例を示す図

【図11】本発明の実施の形態2における機器制御システムの構成例を示す図

【図12】同実施の形態における機器制御システムの家庭内配置例を示す図

【図13】同実施の形態における制御子機部11の構成例を示す図

【図14】同実施の形態における新規被制御機器2を機器制御システムへ登録する処理シーケンスを示す図

【図 15】同実施の形態における被制御機器 2 の機器制御システムからの登録削除シーケンスを示す図

【図 16】本発明の実施の形態 3 における宅外から制御可能な機器制御システムの構成例を示す図

【図 17】同実施の形態における機器制御システムが常に接続の形態でインターネットに接続されている場合のインターネットを通じたアクセス開始シーケンスを示す図

【図 18】同実施の形態における認証情報表の一例を示す図

【図 19】同実施の形態におけるインターネットアクセス部の設定をリセットする処理のシーケンスを示す図

【図 20】同実施の形態における機器制御システムがダイヤルアップの形態でインターネットに接続されている場合のアクセス開始シーケンスを示す図

【図 21】同実施の形態における認証情報表の一例を示す図

【図 22】同実施の形態における機器制御部 204 に実施の形態 2 の機器制御システムを適用した場合の構成例を示す図

【図 23】(a) 同実施の形態における認証情報表の一例を示す図

(b) 同実施の形態におけるサービスクラス定義表を示す図

【図 24】同実施の形態における認証情報表の一例を示す図

【図 25】同実施の形態における認証情報表の一例を示す図

【図 26】同実施の形態における機器制御システムが常時接続の形態でインターネットに接続されている場合のインターネットを通じたアクセス開始シーケンスを示す図

時接続の形態でインターネットに接続されている場合の第 2 のアクセス開始シーケンス例を示す図

【図 27】同実施の形態における認証情報表を示す図

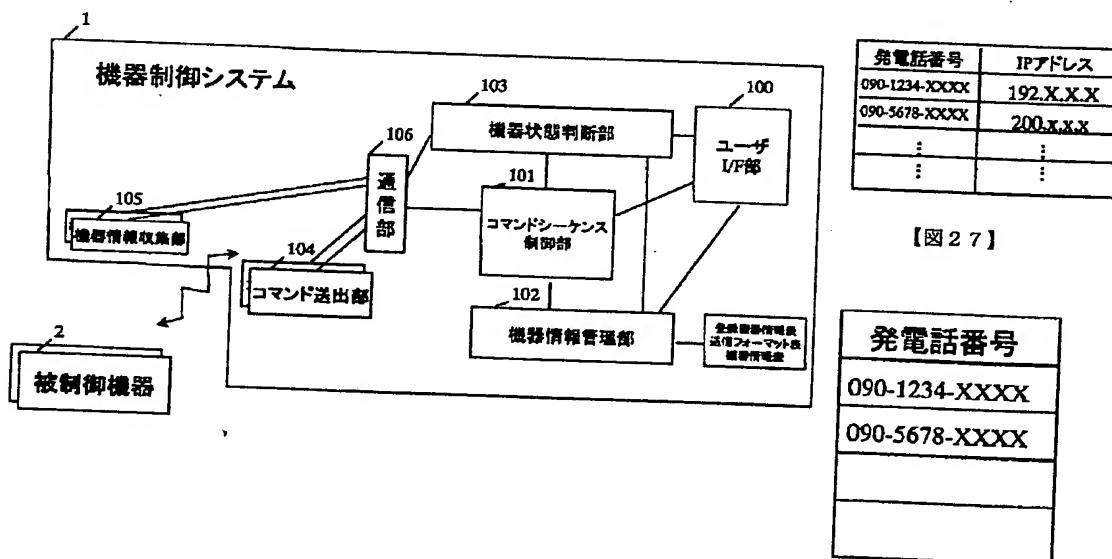
【図 28】同実施の形態におけるコマンドシーケンス制御部がタイマーを予約した時間に実行する処理シーケンスを示す図

#### 【符号の説明】

- 1 機器制御システム
- 2 被制御機器
- 1 0 制御親機部
- 1 1 制御子機部
- 2 0 インターネット網と電話網の両方が利用可能なユーザ端末
- 2 0 a インターネット網を利用するユーザ端末
- 2 0 b 電話網を利用するユーザ端末
- 2 1 インターネット
- 2 2 電話網
- 1 0 0 ユーザ I/F 部
- 1 0 1 コマンドシーケンス制御部
- 1 0 2 機器情報管理部
- 1 0 3 機器状態判断部
- 1 0 4 コマンド送出部
- 1 0 5 機器情報収集部
- 1 0 6 通信部
- 1 0 8 機器登録受付部
- 2 0 1 インターネットアクセス部
- 2 0 2 電話網アクセス部
- 2 0 3 通信情報解析部
- 2 0 4 機器制御部

【図 1】

【図 18】



【図2】

【図24】

## 登録機器情報表

技制御機器名	技制御機器種別	機器情報収集部ID	コマンド送出部ID
1F居間 ビデオ	P社 N型ビデオ	コンセント型1 光センサー型1	コマンド送出部1
1F居間 ビデオ	S社 V型ビデオ	コンセント型2 光センサー型2	コマンド送出部1
1F居間 テレビ	S社 B型テレビ	コンセント型3	コマンド送出部1
1F居間 エアコン	N社 E型エアコン	コンセント型4	コマンド送出部1
1F和室 こたつ	P社 A型こたつ	コンセント型5	—
1F和室 エアコン	N社 C型エアコン	コンセント型6	コマンド送出部2
:	:	:	

免電話番号	ユーザ名	パスワード
090-1234-XXXX	HANAKO	*****
090-5678-XXXX	TAROU	*****
:	:	
:	:	

【図3】

## 送信フォーマット表

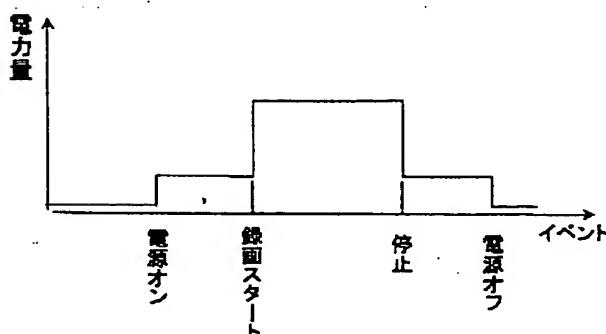
種別	キャリア周波数	コード差	コードフォーマット	信号ストラクチャ
P社-1	xx kHz	xx bit	.....	.....
P社-2				
N社-1	:	:	:	:
:	:	:	:	:

## 機器情報表

機器	送信フォーマット 概要	制御用コマンドコード	状態解析用情報
P社 A型こたつ	—	—	コンセント型) ON:xx A OFF: 0A
P社 N型ビデオ	P社-1	Power:xx 再生:xx 停止:xx 早送り:xx ...	コンセント型) ON:xx A OFF: xx A 録画:xx A... 光センサー型) 再生:(A) xx A 録画:(0) xx A ...
P社 S型ビデオ	P社-2	—	—
S社 V型ビデオ	S社-1	—	—
P社 T型テレビ	P社-1	Power:XX 音量:XX 音量down:XX ...	コンセント型) ON:xx A OFF: 0A ...
S社 B型テレビ	S社-2	—	—
:	:	:	:
N社 E型エアコン	N社-1	Power:xx 運転切り替え:XX ...	コンセント型) ON:xx A OFF: 0A ...
:	:	:	:

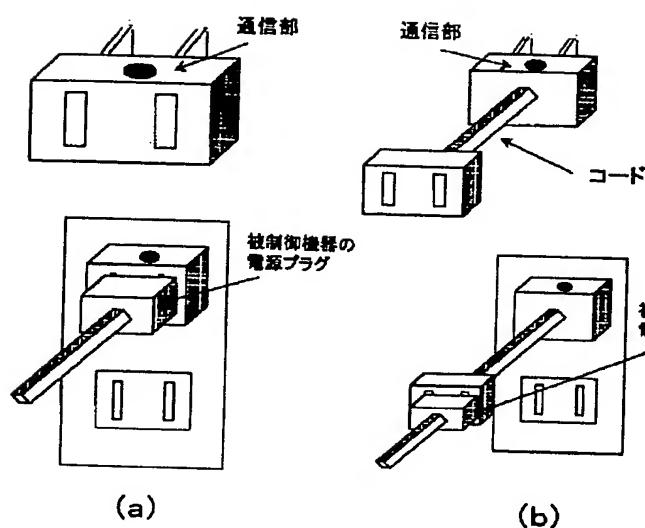
【図6】

【図21】



免電話番号	IPアドレス	メールアドレス
090-1234-XXXX	192.X.X.X	hanako@hi-ho.ne.jp
090-5678-XXXX	200.X.X.X	taro@hi-ho.ne.jp
:	:	
:	:	

【図4】



【図23】

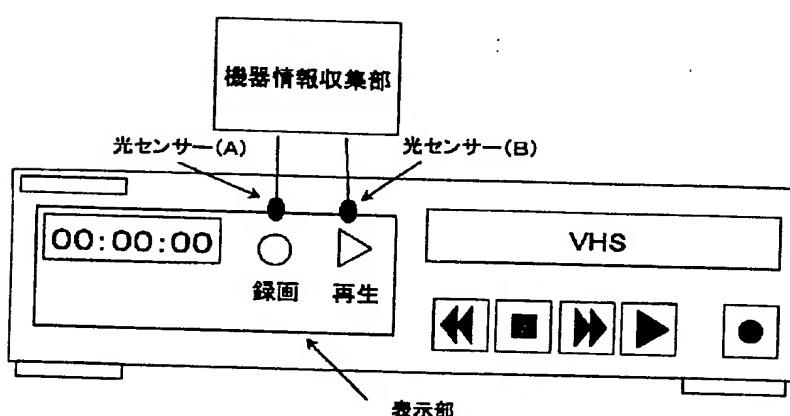
発電話番号	サービスクラス
090-1234-XXXX	管理者
090-5678-XXXX	一般ユーザ
⋮	ゲスト
⋮	⋮

(a)

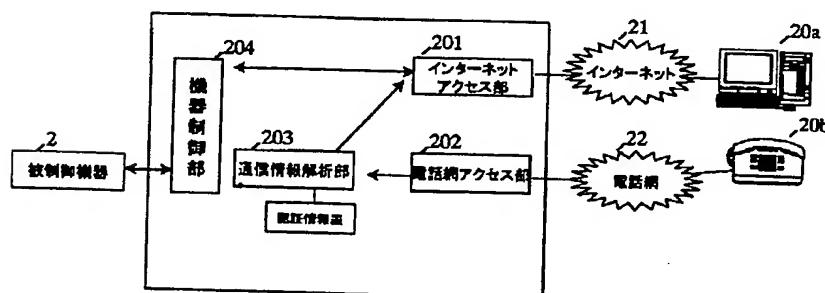
サービスクラス	サービス内容		
	実施対象	操作制限	状態表示
管理者	○	○	○
一般ユーザ	×	○	○
ゲスト	×	×	○
⋮			

(b)

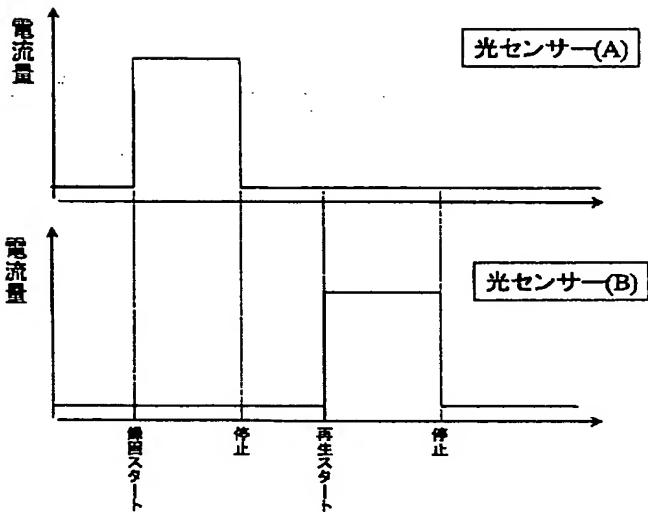
【図5】



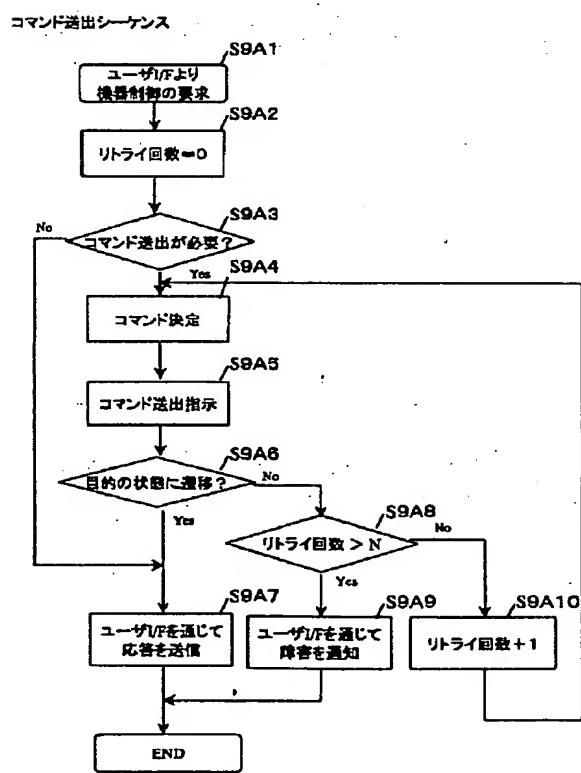
【図16】



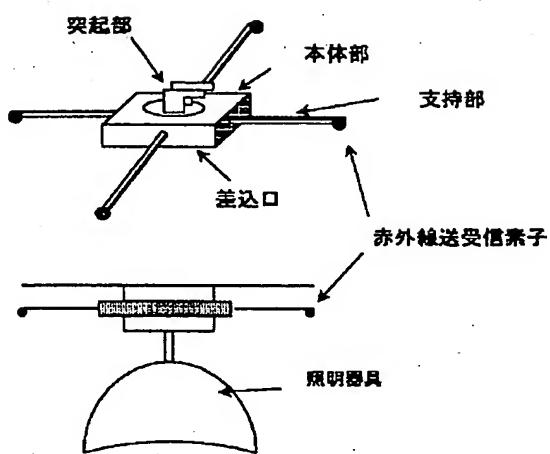
【図7】



【図9】

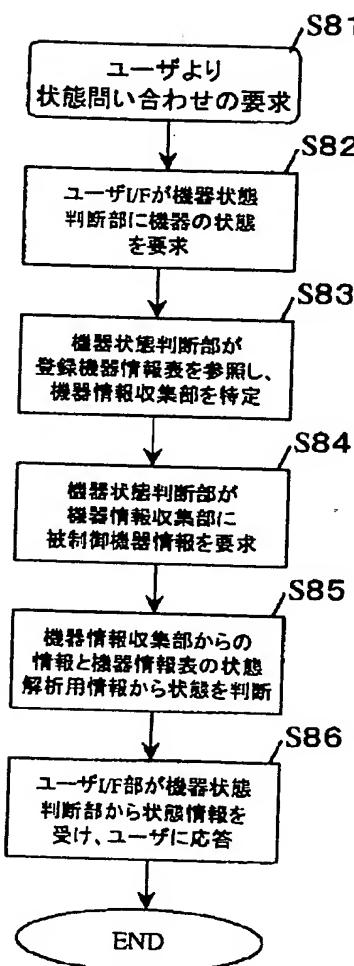


【図13】

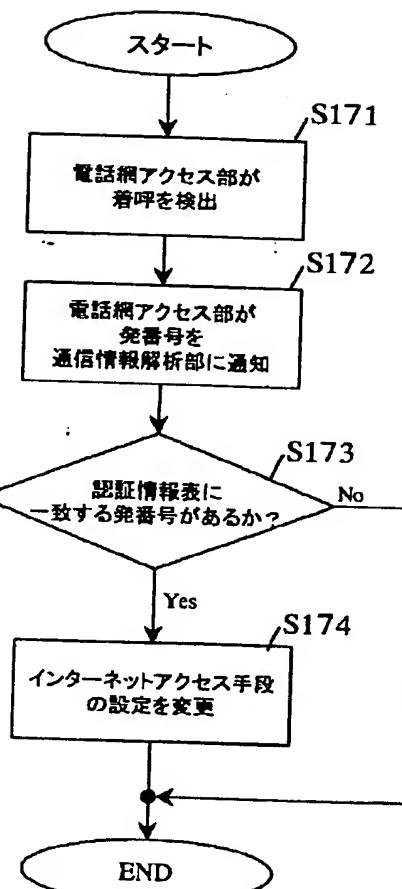


【図 8】

## 状態問い合わせシーケンス



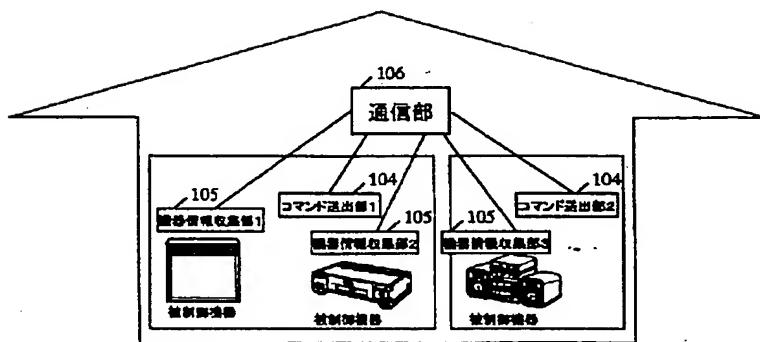
【図 17】



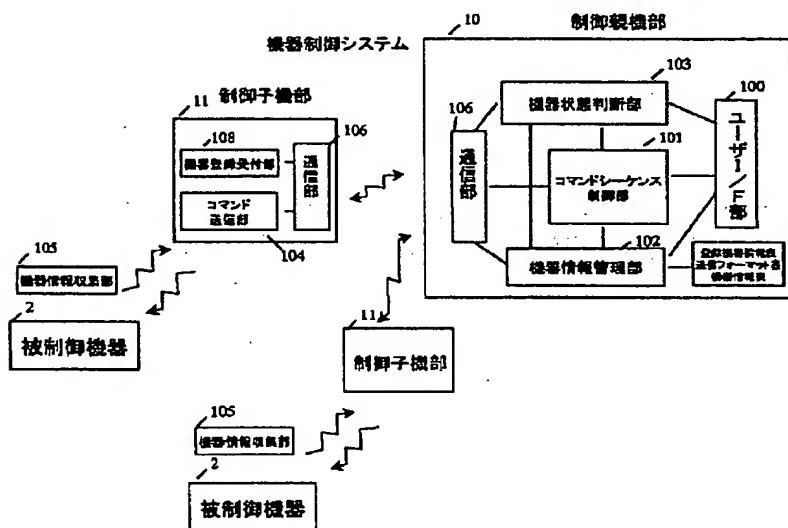
【図 25】

発電話番号	IPアドレス	ユーザ名	パスワード	サービスクラス
090-1234-XXXX	192.X.XX	HANAKO	*****	管理者
090-3678-XXXX	200.X.XX	TAROU	*****	一般ユーザ
:	:	:	:	ゲスト
:	:	:	:	:

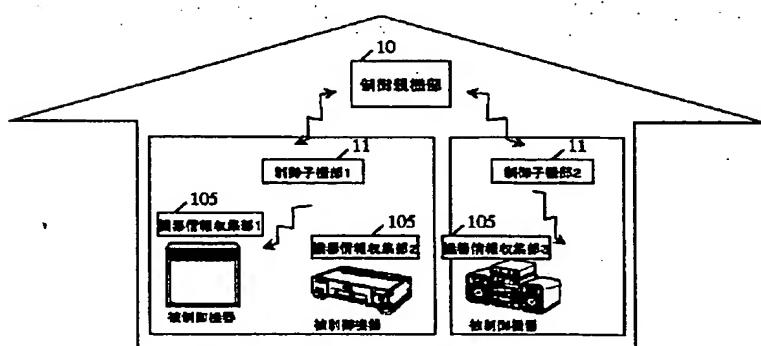
【図 1 0】



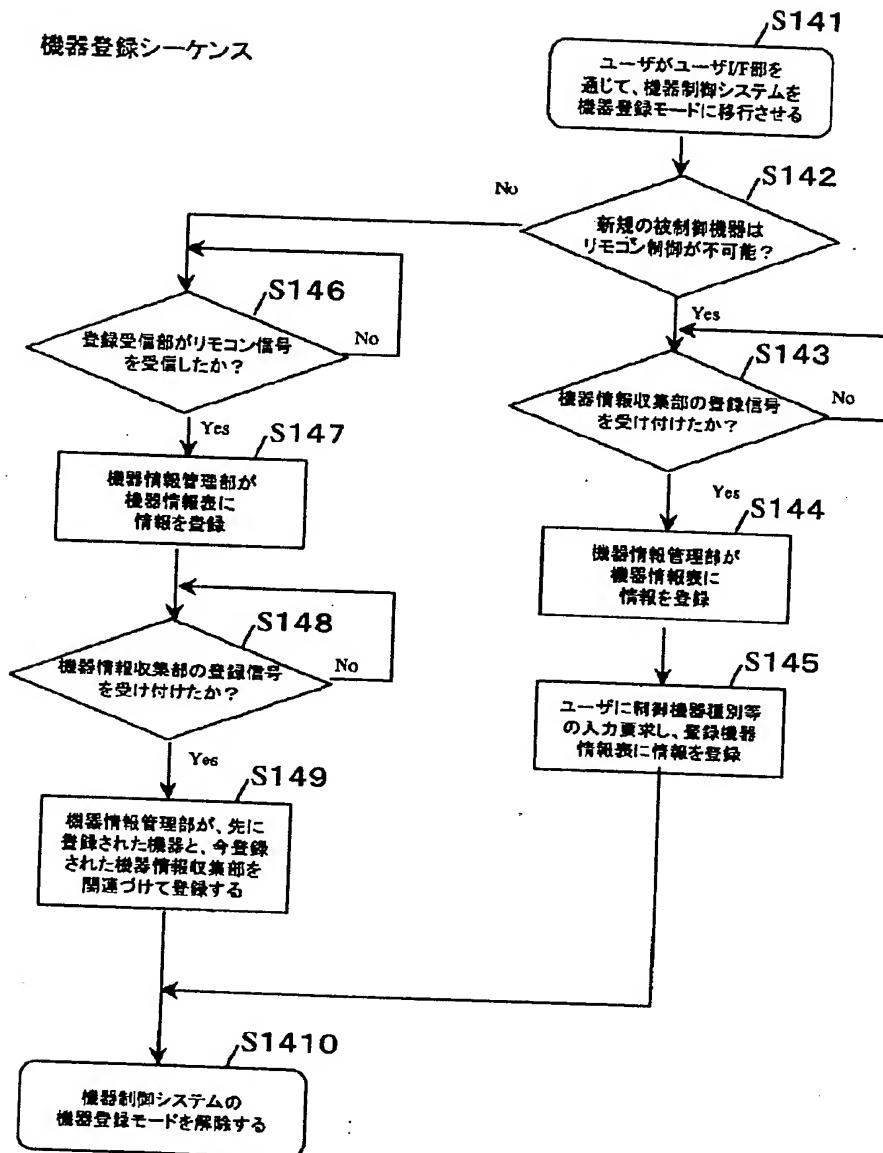
【図 1 1】



【図 1 2】

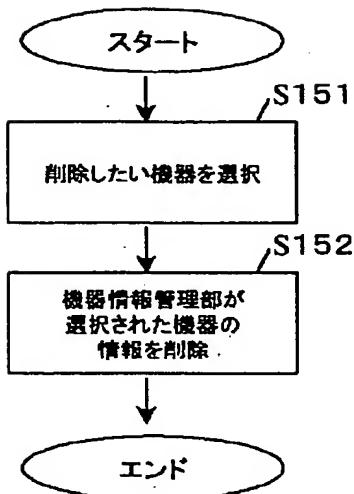


【図14】

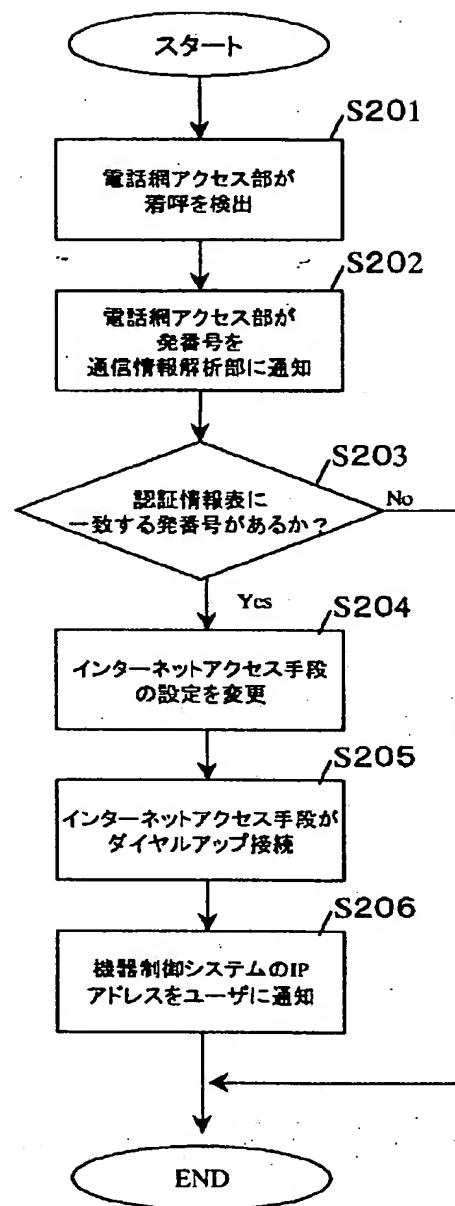


【図15】

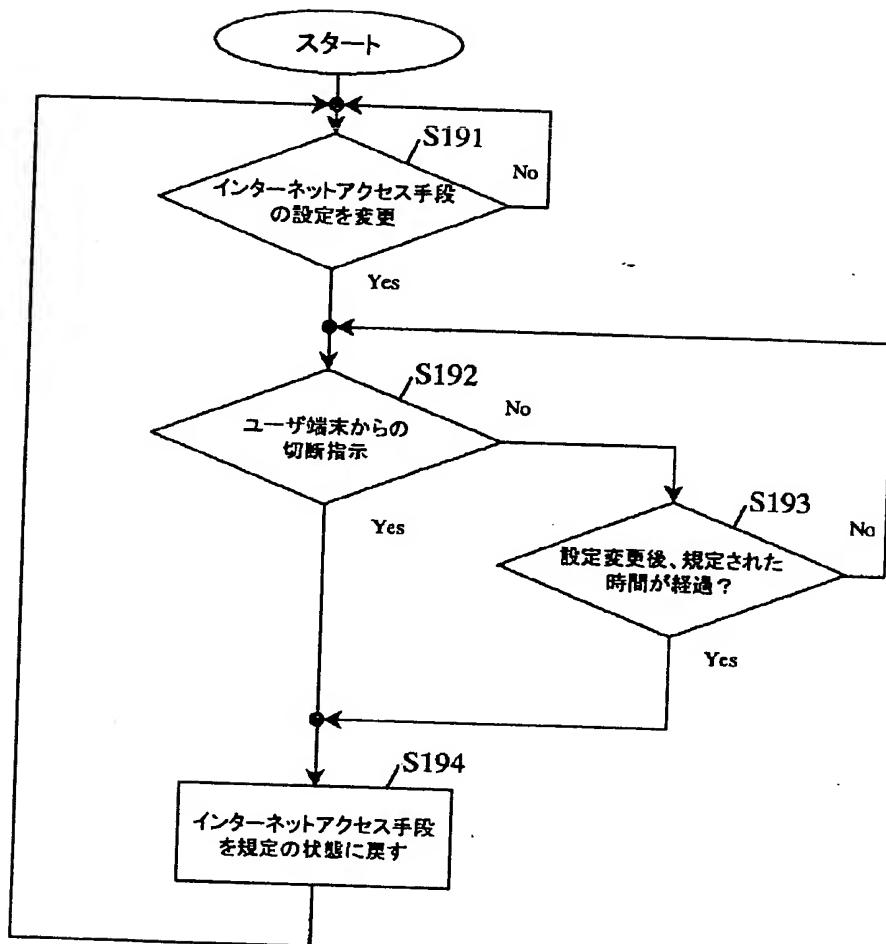
## 削除シーケンス



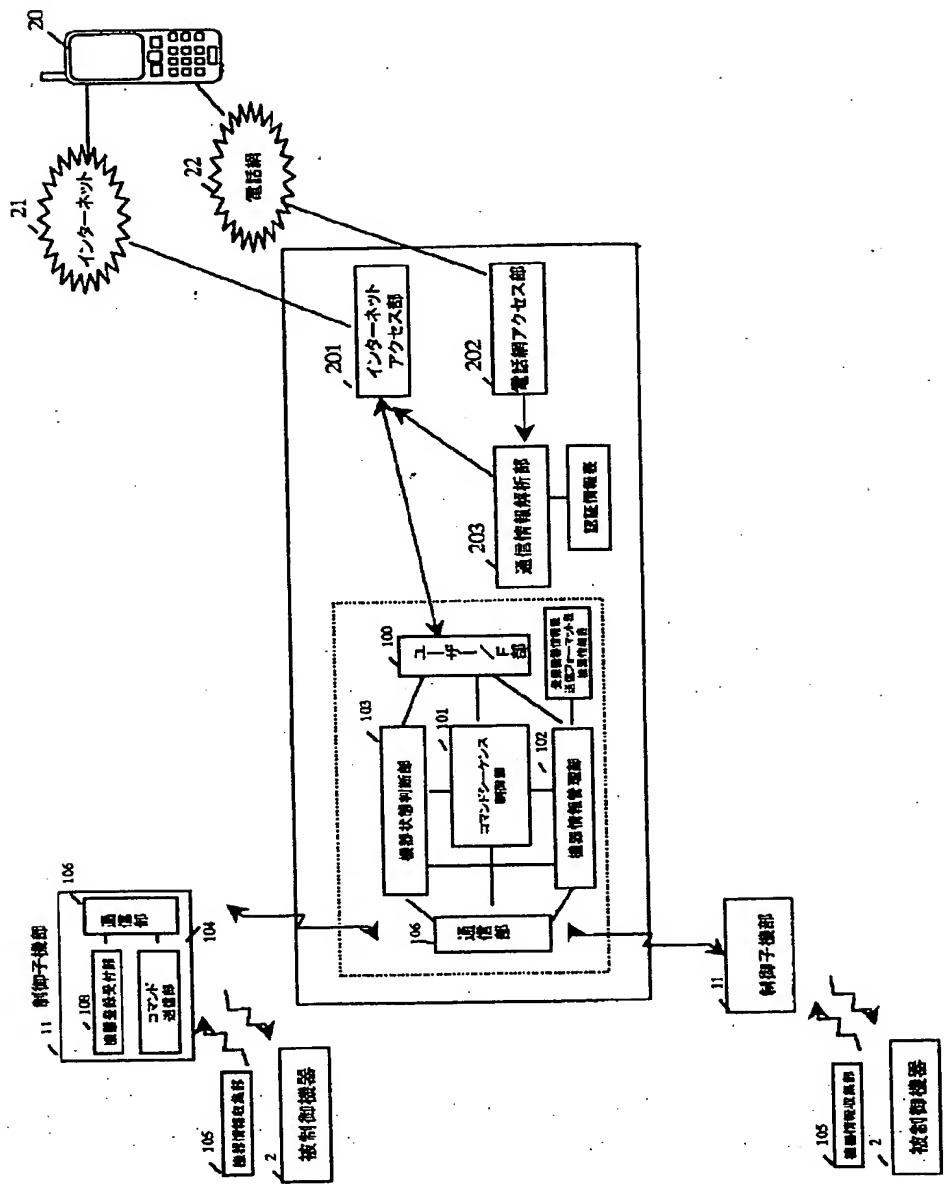
【図20】



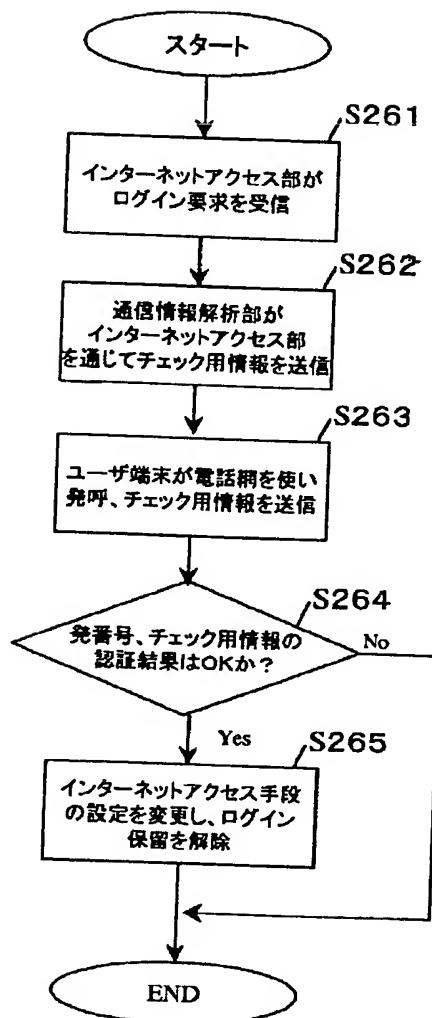
【図19】



[图22]

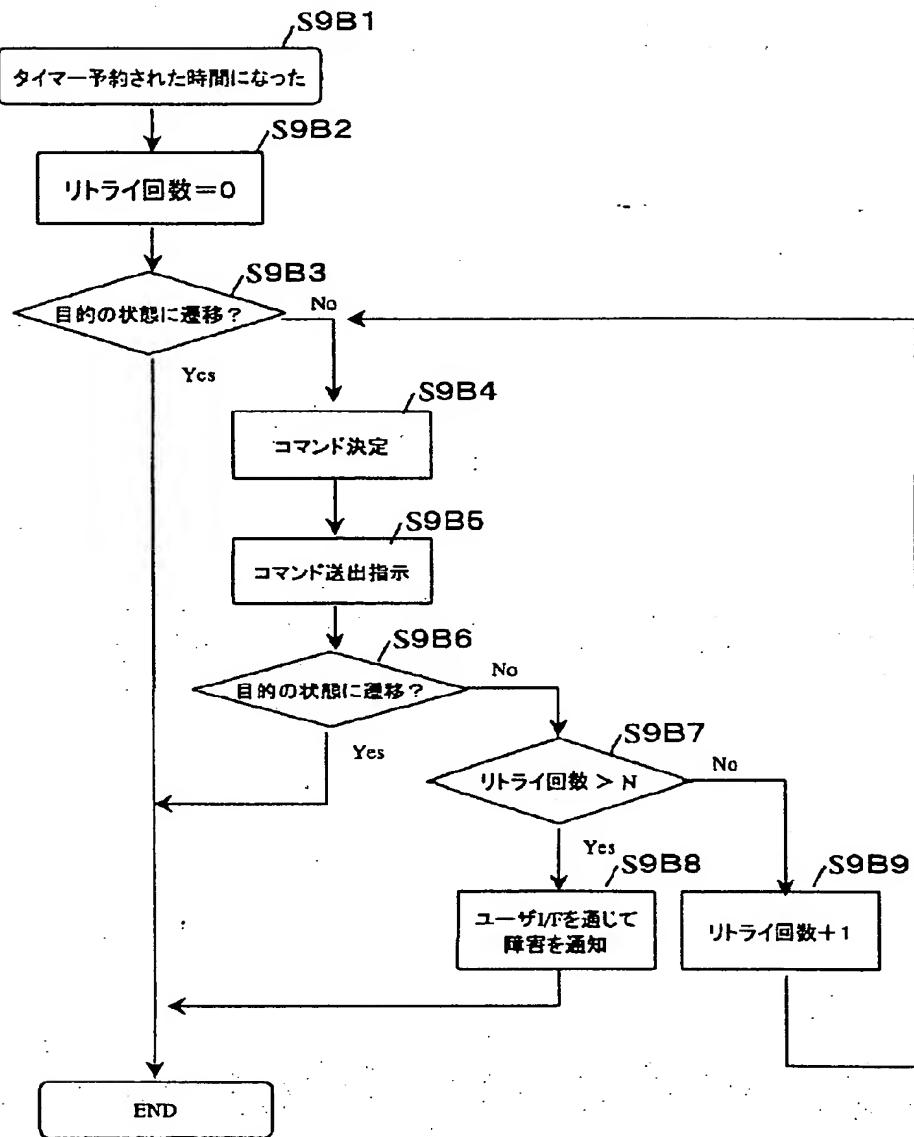


【図26】



【図28】

コマンド送出シーケンス(タイマー編)



フロントページの続き

(51) Int. Cl. <sup>7</sup>

H 04 N 5/00

識別記号

F I  
H 04 N 5/00

テーマコード(参考)

A

F ターム(参考) 5B085 CA04 CC01  
5B089 GA23 GB02 HA10 JA35 JA36  
JB10 JB15 KB06 KC57 KE02  
KE03  
5C056 AA05 AA07 BA10 CA06 CA13  
CA19 CA20 DA11  
5K048 AA06 AA15 BA01 BA04 DB04  
DC07 EB02 EB10 EB12 HA01  
HA02 HA04 HA06  
5K101 KK11 LL01 PP04